(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年10 月7 日 (07.10.2004)

PCT

(10) 国際公開番号
WO 2004/086233 A1

(51) 国際特許分類[7]: G06F 12/14, G11B 20/10, H04L 9/08

(21) 国際出願番号: PCT/JP2004/003579

(22) 国際出願日: 2004 年3 月17 日 (17.03.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-085500 2003 年3 月26 日 (26.03.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 浅野 智之 (ASANO, Tomoyuki) [JP/JP]; 〒1410001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 宮田 正昭, 外(MIYATA, Masaaki et al.); 〒1040041 東京都中央区新富一丁目1番7号 銀座ティーケイビル 澤田・宮田・山田特許事務所 Tokyo (JP).

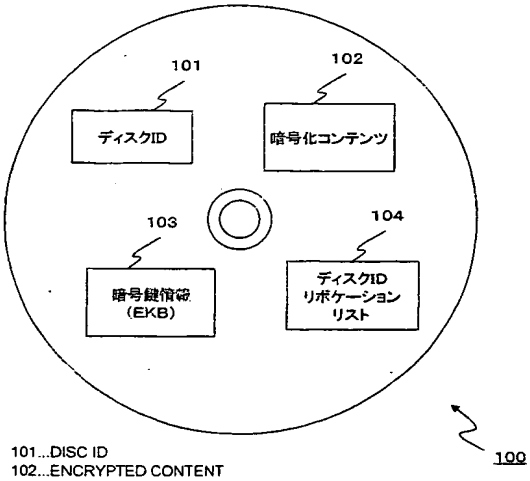
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL,

[続葉有]

(54) Title: INFORMATION RECORDING MEDIUM, INFORMATION PROCESSING DEVICE, INFORMATION RECORDING MEDIUM MANUFACTURING DEVICE, AND METHOD, AND COMPUTER PROGRAM

(54) 発明の名称: 情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びにコンピュータ・プログラム



101...DISC ID
102...ENCRYPTED CONTENT
103...ENCRYPTION KEY INFORMATION (EKB)
104...DISC ID REVOCATION LIST

(57) Abstract: There are provided an information recording medium, an information processing device, and method capable of excluding flood and use of unauthorized copying of a content according to information recording medium management. An information recording medium containing an encrypted content stores an information recording medium ID as an identifier unique to the information recording medium and an information recording medium ID revocation list as a list of information recording medium ID's which have been judged to be unauthorized. An information processing device for reading out and reproducing a content stored in an information recording medium executes reproduction of a content only when the information recording medium ID stored in the information recording medium does not match with any of revoke information recording medium ID's described in the information recording medium ID revocation list. With this configuration, it is possible to exclude flood and use of unauthorized copying of a content.

[続葉有]

WO 2004/086233 A1

SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 情報記録媒体の管理に基づいてコンテンツの不正コピーの氾濫、利用を排除を実現した情報記録媒体、情報処理装置および方法を提供する。暗号化コンテンツを格納した情報記録媒体に、情報記録媒体固有の識別子である情報記録媒体ＩＤと、不正であると判定された情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストとを格納し、情報記録媒体に格納されたコンテンツを読み出して再生する情報処理装置において、情報記録媒体に格納された情報記録媒体ＩＤが、情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと一致しないことを条件としてコンテンツ再生処理を実行する構成とした。本構成により、コンテンツの不正コピーの氾濫、利用を排除することが可能となる。

明 細 書

情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びにコンピュータ・プログラム

技術分野

本発明は、情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、ＣＤ、ＤＶＤ、ＭＤ等、各種のコンテンツ記録媒体に、記録媒体識別子を格納し、不正記録媒体のリストとしてのリボケーションリストに基づくコンテンツ利用制御を行うことにより、不正コピーコンテンツを格納したＣＤ－Ｒディスク等の氾濫、利用の防止を実現する情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びにコンピュータ・プログラムに関する。

背景技術

昨今、音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはＣＤ(Compact Disc)、ＤＶＤ(Digital Versatile Disk)、ＭＤ(Mini Disk)等の情報記録媒体（メディア）を介して流通している。これらの流通コンテンツは、ユーザの所有するＰＣ（Personal Computer)、ＣＤプレーヤ、ＤＶＤプレーヤ、ＭＤプレーヤ等の再生装置、あるいはゲーム機器等において再生され利用される。

音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテ

ンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。

特に、近年においては、情報をデジタル的に記録する記録装置や記憶媒体が普及しつつある。このようなデジタル記録装置および記憶媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができる。現実問題として、コンテンツをＣＤ－Ｒ等にコピーした、いわゆる海賊版ディスクが大量に流通しているという問題がある。

このように、コピーが違法に行われた記憶媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。

発明の開示

本発明は、上述の問題点に鑑みてなされたものであり、コピーが違法に行われた記憶媒体からのコンテンツ再生、コンテンツ利用の実行を制限することを可能とした情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

本発明は、ＣＤ、ＤＶＤ、ＭＤ等、各種のコンテンツ記録媒体に、記録媒体識別子を格納し、不正記録媒体のリストとしてのリボケーションリストに基づくコンテンツ利用制御を行うことにより、不正コピーコンテンツを格納したＣＤ－Ｒ等の情報記録媒体の利用を制御することで、コピーが違法に行われた記憶媒体からのコンテンツ再生、コンテンツ利用の実行を制限することを可能とした情報記録媒体、情報処理装置、情報記録媒体製造装置、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

本発明の第１の側面は、

情報記録媒体であり、

暗号化コンテンツと、

前記暗号化コンテンツの復号処理に必要とする暗号鍵情報と、

情報記録媒体固有の識別子である情報記録媒体ＩＤと、

不正であると判定された情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストと、

を格納したことを特徴とする情報記録媒体にある。

さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体ＩＤリボケーションリストは、該情報記録媒体ＩＤリボケーションリストの格納データの改竄の有無を判定するための改竄検証値を持つ構成であることを特徴とする。

さらに、本発明の情報記録媒体の一実施態様において、前記暗号鍵情報は、前記暗号化コンテンツの復号に適用する鍵を取得可能な暗号化鍵データとしての有効化キーブロック（ＥＫＢ：Enabling Key Block）を含む構成であることを特徴とする。

さらに、本発明の情報記録媒体の一実施態様において、前記有効化キーブロック（ＥＫＢ：Enabling Key Block）は、前記情報記録媒体の利用デバイスである情報処理装置に階層型鍵配信ツリー構成を適用して提供された鍵情報としてのデバイスノードキー（ＤＮＫ：Device Node Key）に基づいて復号処理の可能な暗号鍵情報であることを特徴とする。

さらに、本発明の第２の側面は、

コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実行する情報処理装置であり、

不正であると判定された情報記録媒体ＩＤのリストである情報記録媒体Ｉ

Ｄリボケーションリストを格納したメモリを有し、

情報記録媒体に格納された情報記録媒体ＩＤと前記メモリに格納された情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤとの照合処理を実行し、情報記録媒体に格納された情報記録媒体ＩＤが、情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと一致しないことを条件としてコンテンツ再生処理を実行する構成を有することを特徴とする情報処理装置にある。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストの改竄検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョン比較を実行し、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストのバージョンがメモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョンより新しいものである場合に、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストをメモリに格納するリスト更新処理を実行する構成であることを特徴とする。

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、階層型鍵配信ツリー構成を適用して提供された鍵情報としてのデバイスノードキー（ＤＮＫ：Device Node Key）を有し、前記情報記録媒体に格納された暗号化鍵情報としての有効化キーブロック（ＥＫＢ：Enabling Key Block）を前記デバイスノードキー（ＤＮＫ：Device Node Key）に基づいて復号し、前記情報記録媒体に格納された暗号化コンテンツの復号に適用する鍵の取得処理を実行する構成であることを特徴とする。

さらに、本発明の第３の側面は、

情報記録媒体を製造する情報記録媒体製造装置であり、

暗号化コンテンツと、

前記暗号化コンテンツの復号処理に必要とする暗号鍵情報と、

不正であると判定された情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストとを情報記録媒体に記録するとともに、

情報記録媒体固有の識別子である情報記録媒体ＩＤを製造する情報記録媒体毎に変更して記録する処理を実行する構成を有することを特徴とする情報記録媒体製造装置にある。

さらに、本発明の情報記録媒体製造装置の一実施態様において、前記情報記録媒体ＩＤリボケーションリストは、該情報記録媒体ＩＤリボケーションリストの格納データの改竄の有無を判定するための改竄検証値を持つ構成であることを特徴とする。

さらに、本発明の情報記録媒体製造装置の一実施態様において、前記暗号鍵情報は、前記暗号化コンテンツの復号に適用する鍵を取得可能な暗号化鍵データとしての有効化キーブロック（ＥＫＢ：Enabling Key Block）を含む構成であることを特徴とする。

さらに、本発明の第４の側面は、

コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実行する情報処理方法であり、

情報記録媒体に格納された情報記録媒体ＩＤを読み出すステップと、

情報処理装置内のメモリに格納された不正情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと、前記情報記録媒体に格納された情報記録媒体ＩＤとの照合処理を実行するステップと、

情報記録媒体に格納された情報記録媒体ＩＤが、情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと一致しないことを条件としてコンテンツ再生処理を実行するステップと、

を有することを特徴とする情報処理方法にある。

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストの改竄検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョン比較を実行し、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストのバージョンがメモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョンより新しいものである場合に、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストをメモリに格納するリスト更新処理を実行するステップを有することを特徴とする。

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、階層型鍵配信ツリー構成を適用して提供された鍵情報としてのデバイスノードキー（ＤＮＫ：Device Node Key）を適用して、前記情報記録媒体に格納された暗号化鍵情報としての有効化キーブロック（ＥＫＢ：Enabling Key Block）を復号し、前記情報記録媒体に格納された暗号化コンテンツの復号に適用する鍵の取得処理を実行するステップを有することを特徴とする。

さらに、本発明の第５の側面は、

情報記録媒体を製造する情報記録媒体製造方法であり、

暗号化コンテンツと、前記暗号化コンテンツの復号処理に必要とする暗号鍵情報と、不正であると判定された情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストとを情報記録媒体に記録するステップと、

情報記録媒体固有の識別子である情報記録媒体ＩＤを製造する情報記録媒体毎に変更して記録する処理を実行するステップと、

を有することを特徴とする情報記録媒体製造方法にある。

さらに、本発明の第６の側面は、

コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実行する

コンピュータ・プログラムであり、

情報記録媒体に格納された情報記録媒体ＩＤを読み出すステップと、

情報処理装置内のメモリに格納された不正情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと、前記情報記録媒体に格納された情報記録媒体ＩＤとの照合処理を実行するステップと、

情報記録媒体に格納された情報記録媒体ＩＤが、情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと一致しないことを条件としてコンテンツ再生処理を実行するステップと、

を有することを特徴とするコンピュータ・プログラムにある。

本発明の構成に従えば、情報記録媒体に、暗号化コンテンツと、暗号化コンテンツの復号処理に必要とする暗号鍵情報と、情報記録媒体固有の識別子である情報記録媒体ＩＤと、不正であると判定された情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストとを格納した構成とし、情報記録媒体に格納されたコンテンツを読み出して再生する情報処理装置において、情報記録媒体に格納された情報記録媒体ＩＤが、情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと一致しないことを条件としてコンテンツ再生処理を実行する構成としたので、不正コピーコンテンツの格納媒体に記録された情報記録媒体ＩＤを情報記録媒体ＩＤリボケーションリストに記述することで、リスト化されたＩＤを持つディスクの再生が防止され、コンテンツの不正コピーの氾濫、利用を排除することが可能となる。

また、本発明の構成では、情報処理装置において、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストの改竄検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョン比較を実行し、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストのバージョンがメモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョンより新しいものである場合に、情報

記録媒体に格納された情報記録媒体ＩＤリボケーションリストをメモリに格納するリスト更新処理を実行する構成としたので、随時更新されたリストによるコンテンツ再生制御の実行が可能となる。

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

図面の簡単な説明

図１は、情報記録媒体の格納データについて説明する図である。

図２は、情報記録媒体に格納される情報記録媒体（ディスク）ＩＤリボケーションリスト（ＤＩＲＬ）のデータ構成を説明する図である。

図３は、ＭＡＣ値生成処理例を示す図である。

図４は、各種キー、データの暗号化処理、配布処理について説明するツリー構成図である。

図５は、各種キー、データの配布に使用される有効化キーブロック（ＥＫＢ）の例を示す図である。

図６は、コンテンツ鍵の有効化キーブロック（ＥＫＢ）を使用した配布例と復号処理例を示す図である。

図７は、有効化キーブロック（ＥＫＢ）のフォーマット例を示す図である。

図８は、有効化キーブロック（ＥＫＢ）のタグの構成を説明する図である。

図９は、ツリー構成におけるカテゴリ分割を説明する図である。

図１０は、ツリー構成におけるカテゴリ分割を説明する図である。

図１１は、情報処理装置の構成を示すブロック図である。

図１２は、情報処理装置の実行する処理を示すフローチャート図である。

図１３は、情報処理装置の実行するリボーク判定処理を示すフローチャート図である。

図１４は、情報処理装置の実行するコンテンツ再生処理を示すフローチャート図である。

図１５は、情報記録媒体の製造および管理構成について説明する図である。

図１６は、情報記録媒体製造装置の構成例を示す図である。

図１７は、情報記録媒体の製造処理を示すフローチャート図である。

発明を実施するための最良の形態

以下、本発明の情報記録媒体、情報処理装置、および方法、並びにコンピュータ・プログラムについて詳細に説明する。

［１．情報記録媒体］

まず、図１以下を参照して、本発明に係る情報記録媒体のデータ記録構成例について説明する。図１は、ＣＤ(Compact Disc)、ＤＶＤ(Digital Versatile Disk)、ＭＤ(Mini Disk)その他フラッシュメモリ等、各種の情報記録媒体１００の格納データについて説明する図である。図１にはディスク状の媒体を例として示してあるが、本発明はディスク状の媒体に限らず、フラッシュメモリ等の各種の情報記録媒体において適用可能である。

情報記録媒体１００には、図１に示す情報が格納されている。ディスクＩＤ

１０１はディスク個別の識別子であり、消去や書き換えが困難であるように格納される。なお、以下に説明する実施例では、ディスク状の媒体をコンテンツ格納情報記録媒体の例として示しているので、その識別子をディスクＩＤとして説明する。フラッシュメモリ等の各種の情報記録媒体をコンテンツ格納情報記録媒体として利用した場合はディスクＩＤに対応する情報記録媒体ＩＤが設定される。

暗号化コンテンツ１０２は暗号化されたコンテンツであり、暗号化コンテンツ１０２を復号するためのコンテンツ鍵は、例えば階層型キー配信構成によって、正当なコンテンツ利用機器としての情報処理装置に提供されるデバイスノードキー（ＤＮＫ：Device Node Key）に基づいて、情報記録媒体１００に格納された暗号鍵情報である有効化キーブロック（ＥＫＢ：Enabling Key Block）１０３の復号処理等によってコンテンツ鍵を取得することができる。

階層型キー配信構成によるデバイスノードキー（ＤＮＫ）の提供、およびデバイスノードキー（ＤＮＫ）に基づく有効化キーブロック（ＥＫＢ）の復号処理による鍵取得処理の詳細については後述する。

また、情報記録媒体１００上にはディスクＩＤリボケーションリスト（ＤＩＲＬ:Disc ID Revocation List）１０４が格納される。ディスクＩＤリボケーションリスト（ＤＩＲＬ:Disc ID Revocation List）１０４は、不正コピー等が行われたと認定されたディスク、例えば市場に不正なコピーコンテンツを格納したＣＤ－Ｒが発見された場合に、その不正ＣＤ－ＲにコンテンツとともにコピーされたディスクＩＤを抽出し、リスト化したデータである。ディスクＩＤリボケーションリスト（ＤＩＲＬ:Disc ID Revocation List）１０４の生成、管理、ディスク製造者に対するリスト情報提供は、特定の信頼される管理局（ＣＡ：Central Authority）が実行する。

ディスクＩＤリボケーションリスト（ＤＩＲＬ:Disc ID Revocation List）

のデータ構成について、図２を参照して説明する。ディスクＩＤリボケーションリスト（ＤＩＲＬ:Disc ID Revocation List）１５０は、図２に示すように、ディスクＩＤリボケーションリスト（ＤＩＲＬ:Disc ID Revocation List）が作成された時期により単調増加するバージョン番号１５１と、排除すべきディスクのディスクＩＤを羅列したリボークディスクＩＤリスト１５２と、バージョン番号１５１とリボークディスクＩＤリスト１５２に対する改竄検証値１５３としての認証子が含まれる。改竄検証値１５３は、対象となるデータ、この場合はバージョン番号１５１とリボークディスクＩＤリスト１５２が改竄されているか否かを判別するために適用するデータであり、公開鍵暗号技術を用いたデジタル署名や、共通鍵暗号技術を用いたメッセージ認証コード（ＭＡＣ：Message Authentication Code）が適用される。

改竄検証値１５３として公開鍵暗号技術を用いたデジタル署名を用いる際には、信頼できる機関、例えば上述の管理局（ＣＡ：Central Authority）の署名検証鍵（公開鍵）を再生機が取得し、管理局（ＣＡ：Central Authority）の署名生成鍵（秘密鍵）を用いて作られた署名を各再生機が取得した署名検証鍵（公開鍵）によって検証することで、バージョン番号１５１とリボークディスクＩＤリスト１５２が改竄されているか否かを判別する。

改竄検証値１５３としてメッセージ認証コード（ＭＡＣ：Message Authentication Code）を用いた際のＭＡＣ生成、検証処理について、図３を参照して説明する。メッセージ認証コード（ＭＡＣ：Message Authentication Code）は、データの改竄検証用のデータとして生成されるものであり、ＭＡＣ生成処理、検証処理態様には様々な態様が可能であるが、１例としてＤＥＳ暗号処理構成を用いたＭＡＣ値生成例を図３に示す。

図３に示すように、対象となるメッセージ、この場合は、図２に示すバージョン番号１５１とリボークディスクＩＤリスト１５２を８バイト単位に分割し、（以下、分割されたメッセージをＭ１、Ｍ２、・・・、ＭＮとする）、まず、

初期値（Initial Value（以下、ＩＶとする））とＭ１を排他的論理和する（その結果をＩ１とする）。次に、Ｉ１をＤＥＳ暗号化部に入れ、鍵（以下、Ｋ１とする）を用いて暗号化する（出力をＥ１とする）。続けて、Ｅ１およびＭ２を排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部へ入れ、鍵Ｋ１を用いて暗号化する（出力Ｅ２）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたＥＮがメッセージ認証符号（ＭＡＣ（Message Authentication Code））となる。

ＭＡＣ値は、その生成元データが変更されると、異なる値となり、検証対象のデータ（メッセージ）に基づいて生成したＭＡＣと、記録されているＭＡＣとの比較を行い、一致していれば、検証対象のデータ（メッセージ）は変更、改竄がなされていないことが証明される。

ＭＡＣ生成における鍵Ｋ１としては、たとえば、階層型キー配信構成によるデバイスノードキー（ＤＮＫ）に基づく有効化キーブロック（ＥＫＢ）の復号処理によって得られる鍵（ルートキー）を適用することが可能である。また、初期値ＩＶとしては、予め定めた値を用いることが可能である。

［２．階層型鍵配信ツリー構成］

次に、ブロードキャストエンクリプション（Broadcast Encryption）方式の一態様である階層型鍵配信ツリー構成に従った鍵提供処理、再生機としての情報処理装置管理構成について説明する。

図４の最下段に示すナンバ０～１５がコンテンツ利用を行なう情報処理装置としてのユーザデバイスである。すなわち図４に示す階層ツリー（木）構造の各葉（リーフ：leaf）がそれぞれのデバイスに相当する。

各デバイス０～１５は、製造時あるいは出荷時、あるいはその後において、図４に示す階層ツリー（木）構造における自分のリーフからルートに至るまで

のノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセット（デバイスノードキー（ＤＮＫ：Device Node Key））をメモリに格納する。図４の最下段に示すＫ００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲ（ルートキー）から、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

図４に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図４のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図４のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたＤＶＤ、ＣＤ、ＭＤ、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図４に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図４の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いる１つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダからネットワークまたはＣＤ等の情報記録媒体に格納して提供したり、各デバイス共通に使用するコンテンツ鍵を送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払デー

タをやはり暗号化して出力するといった処理が実行される。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なうエンティテイは、図４の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行可能となる。このようなグループは、図４のツリー中に複数存在する。

なお、ノードキー、リーフキーは、ある１つの鍵管理センター機能を持つ管理システムによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センター機能を持つ管理システム、プロバイダ、決済機関等が実行可能である。

このツリー構造において、図４から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はデバイスノードキー（ＤＮＫ：Device Node Key）として共通のキーＫ００、Ｋ０、ＫＲを含むデバイスノードキー（ＤＮＫ：Device Node Key）を保有する。このノードキー共有構成を利用することにより、例えば共通のキーをデバイス０，１，２，３のみに提供することが可能となる。たとえば、共通に保有するノードキーＫ００は、デバイス０，１，２，３に共通する保有キーとなる。また、新たなキーＫｎｅｗをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Ｋｎｅｗ）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Ｋｎｅｗ）を解いて新たなキーＫｎｅｗを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１，Ｋ００

１，Ｋ００，Ｋ０，ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１，Ｋ００，Ｋ０，ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

更新キーの配布処理ついて説明する。キーの更新は、例えば、図５（Ａ）に示す有効化キーブロック（ＥＫＢ：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。なお、有効化キーブロック（ＥＫＢ）は、図４に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック（ＥＫＢ）は、キー更新ブロック（ＫＲＢ：Key Renewal Block）と呼ばれることもある。

図５（Ａ）に示す有効化キーブロック（ＥＫＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図５の例は、図４に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図４から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

図５（Ａ）のＥＫＢに示されるようにＥＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノ

ードキーK（t）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、K（t）００１を得ることができる。また、復号により得たK（t）００１を用いて、図５（A）の下から２段目の暗号化キーEnc（K（t）００１，K（t）００）を復号可能となり、更新ノードキーK（t）００を得ることができる。以下順次、図５（A）の上から２段目の暗号化キーEnc（K（t）００，K（t）０）を復号し、更新ノードキーK（t）０、図５（A）の上から１段目の暗号化キーEnc（K（t）０，K（t）R）を復号しK（t）Rを得る。一方、デバイスK００００．K０００１は、ノードキーK０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、K（t）００、K（t）０、K（t）Rである。デバイスK００００．K０００１は、図５（A）の上から３段目の暗号化キーEnc（K０００，K（t）００）を復号しK（t）００、を取得し、以下、図５（A）の上から２段目の暗号化キーEnc（K（t）００，K（t）０）を復号し、更新ノードキーK（t）０、図５（A）の上から１段目の暗号化キーEnc（K（t）０，K（t）R）を復号しK（t）Rを得る。このようにして、デバイス０，１，２は更新した鍵K（t）Rを得ることができる。なお、図５（A）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図４に示すツリー構造の上位段のノードキー：K（t）０，K（t）Rの更新が不要であり、ノードキーK００のみの更新処理が必要である場合には、図５（B）の有効化キーブロック（EKB）を用いることで、更新ノードキーK（t）００をデバイス０，１，２に配布することができる。

図５（B）に示すEKBは、例えば特定のグループにおいて共有する新たなコンテンツ鍵を配布する場合に利用可能である。具体例として、図４に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のコンテンツ鍵K（t）conが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーK００を更新したK（t）００を用いて新たな共通の更新コンテンツ鍵：K（t）conを暗号化したデータEnc（K

（ｔ）００，Ｋ（ｔ）ｃｏｎ）を図５（Ｂ）に示すＥＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

すなわち、デバイス０，１，２はＥＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのキー、例えばコンテンツの暗号化復号化に適用するコンテンツ鍵Ｋ（ｔ）ｃｏｎを得ることが可能になる。

図６に、ｔ時点でのキー、例えばコンテンツの暗号化復号化に適用するコンテンツ鍵Ｋ（ｔ）ｃｏｎをＥＫＢの処理によって取得する処理例を示す。ＥＫＢには、Ｋ（ｔ）００を用いてコンテンツ鍵Ｋ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）と図５（Ｂ）に示すデータとが格納されているとする。ここでは、デバイス０の処理例を示す。

図６に示すように、デバイス０は、記録媒体に格納されている世代：ｔ時点のＥＫＢと自分があらかじめ格納しているノードキーＫ０００を用いて上述したと同様のＥＫＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、復号した更新ノードキーＫ（ｔ）００を用いて暗号化データＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）を復号して更新コンテンツ鍵Ｋ（ｔ）ｃｏｎを取得する。さらに、デバイスは、後にそれを使用するために自分だけが持つリーフキーＫ０００００で暗号化して格納してもよい。

また、別の例として、ツリー構造のノードキーの更新は不必要で、時点ｔでのコンテンツ鍵Ｋ（ｔ）ｃｏｎのみを必要な機器が得られればよい、という場合もある。この場合、下記のような方式とすることができる。

いま、図６の例と同様に、デバイス０、１、２にのみコンテンツ鍵Ｋ（ｔ）ｃｏｎを送りたいとする。このとき、ＥＫＢは、

バージョン（Ｖｅｒｓｉｏｎ）：ｔ

インデックス　暗号化キー

０００　　Ｅｎｃ（Ｋ０００、Ｋ（ｔ）ｃｏｎ）

００１０　　Ｅｎｃ（Ｋ００１０、Ｋ（ｔ）ｃｏｎ）

となる。

デバイス０、１はＫ０００を用いて、またデバイス２はＫ００１０を用いて上記ＥＫＢのうちの１つの暗号文を復号ことによりコンテンツ鍵を得ることができる。このようにすることにより、ノードキーの更新は行えないものの、必要な機器にコンテンツ鍵を与える方法をより効率よく（すなわち、ＥＫＢに含まれる暗号文数を減らしてＥＫＢのサイズを小さくするとともに、管理センタでの暗号化およびデバイスでの復号処理の回数を減らせる）することができる。

図７に有効化キーブロック（ＥＫＢ）のフォーマット例を示す。バージョン２０１は、有効化キーブロック（ＥＫＢ）のバージョンを示す識別子である。なお、バージョンは最新のＥＫＢを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック（ＥＫＢ）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ２０３は、有効化キーブロック（ＥＫＢ）中のデータ部の位置を示すポインタであり、タグポインタ２０４はタグ部の位置、署名ポインタ２０５は署名の位置を示すポインタである。

データ部２０６は、例えば更新するノードキーを暗号化したデータを格納する。例えば図５に示すような更新されたノードキーに関する各暗号化キー等を格納する。

タグ部２０７は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図８を用いて説明する。図８では、データとして先に図５（Ａ）で説明した有効化キーブロック（Ｅ

ＫＢ）を送付する例を示している。この時のデータは、図８の表（ｂ）に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーＫ（ｔ）Ｒが含まれているので、トップノードアドレスはＫＲとなる。このとき、例えば最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図８の（ａ）に示す階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが０、ない場合は１が設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図８（ｃ）に示すデータ列、およびタグ列が構成される。

タグは、データＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）... は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図５で説明した構成のように暗号化データに対応させたノード･インデックスを用いて、例えば、

０：Ｅｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）

００：Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）

０００：Ｅｎｃ（Ｋ（（ｔ）０００，Ｋ（Ｔ）００）

... のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

図７に戻って、ＥＫＢフォーマットについてさらに説明する。署名（Signature）２０８は、有効化キーブロック（ＥＫＢ）を発行した例えば鍵管理センター機能を持つ管理システム、コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等が実行する電子署名である。ＥＫＢを受領したデバイスは署名検証によって正当な有効化キーブロック（ＥＫＢ）発行者が発行した有効化キーブロック（ＥＫＢ）であることを確認する。

ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

図９に階層ツリー構造のカテゴリの分類の一例を示す。図９において、階層ツリー構造の最上段には、ルートキーＫｒｏｏｔ３０１が設定され、以下の中間段にはノードキー３０２が設定され、最下段には、リーフキー３０３が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

ここで、一例として最上段から第M段目のあるノードをカテゴリノード３０４として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の１つのノードを頂点として以下、M＋１段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

例えば図９の第M段目の１つのノード３０５にはカテゴリＡが設定され、このノード以下に連なるノード、リーフはカテゴリＡに区分され、様々なデバイスを含むカテゴリＡ専用のノードまたはリーフとして設定される。すなわち、ノード３０５以下を、カテゴリＡとして区分されるデバイスの関連ノード、およびリーフの集合として定義する。

さらに、M段から数段分下位の段をサブカテゴリノード３０６として設定することができる。例えば図に示すようにカテゴリＡノード３０５の２段下のノードに、カテゴリＡに含まれるサブカテゴリＡａノードとして、[再生専用器]のノードを設定する。さらに、サブカテゴリＡａノードである再生専用器のノード３０６以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード３０７が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる[ＰＨＳ]ノード３０８と[携帯電話]ノード３０９を設定することができる。

さらに、カテゴリ、サブカテゴリは、デバイスの種類、メーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位で設定可能である。例えば１つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器ＸＹＺ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器ＸＹＺにその頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（ＥＫＢ）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

また、コンテンツプロバイダの管理するノードをカテゴリノードとした場合には、コンテンツプロバイダが提供するコンテンツを格納したＣＤ、ＭＤ、ＤＶＤ等の情報記録媒体またはネット配信コンテンツを利用する機器をカテゴリノード以下に設定して、その機器に対してその頂点ノード以下の下段のノードキー、リーフキーを提供することが可能となる。

このように、１つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の１つの頂点ノード

を管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（ＥＫＢ）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

例えば、図１０に示されるように、ツリー構成のシステムで、キー管理が行われる。図１０の例では、８＋２４＋３２段のノードがツリー構造とされ、ルートノードから下位の８段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばフラッシュメモリなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そして、このカテゴリノードのうちの１つのノードに、ライセンスを管理するシステムとして本システム（Ｔシステムと称する）が対応する。

すなわち、このＴシステムのノードよりさらに下の階層の２４段のノードに対応するキーが、ショップサーバ、ライセンスサーバ等の管理エンティテイとしてのサービスプロバイダ、あるいはサービスプロバイダが提供するサービスに適用される。この例の場合、これにより、2^{24}（約１６メガ）のサービスプロバイダあるいはサービスを規定することができる。さらに、最も下側の３２段の階層により、2^{32}（約４ギガ）のユーザ（あるいはユーザデバイス）を規定することができる。最下段の３２段のノードからＴシステムのノードまでのパス上の各ノードに対応するキーが、ＤＮＫ（Device Node Key）を構成し、最下段のリーフに対応するＩＤがリーフＩＤとされる。

例えば、コンテンツを暗号化したコンテンツ鍵は更新されたルートキーＫＲ’によって暗号化され、上位の階層の更新ノードキーは、その直近の下位の階層の更新ノードキーを用いて暗号化され、ＥＫＢ内に配置される。ＥＫＢにおける末端から１つ上の段の更新ノードキーはＥＫＢの末端のノードキーあるいはリーフキーによって暗号化され、ＥＫＢ内に配置される。

ユーザデバイスは、サービスデータに記述されているＤＮＫのいずれかのキーを用いて、コンテンツデータとともに配布されるＥＫＢ内に記述されている直近の上位の階層の更新ノードキーを復号し、復号して得たキーを用いて、ＥＫＢ内に記述されているさらにその上の階層の更新ノードキーを復号する。以上の処理を順次行うことで、ユーザデバイスは、更新ルートキーＫＲ’を得ることができる。

上述したように、ツリーのカテゴリ分類により、１つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定した構成が可能となり、カテゴリ段、あるいはサブカテゴリ段の１つの頂点ノードを管理するメーカー、サービスプロバイダ等がそのノードを頂点とする有効化キーブロック（ＥＫＢ）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が実現される。

［３．情報処理装置の処理］

次に、情報記録媒体に格納されたコンテンツの再生を実行するたとえば再生機等の情報処理装置におけるコンテンツ利用処理について説明する。

図１１は、本発明を適用した情報処理装置５００の一実施例構成を示すブロック図である。情報処理装置５００は、入出力Ｉ／Ｆ(Interface)５２０、ＭＰＥＧ(Moving Picture Experts Group)等の各種符号化データの生成、復号を実行するコーデック５３０、Ａ／Ｄ，Ｄ／Ａコンバータ５４１を備えた入出力Ｉ／Ｆ(Interface)５４０、暗号処理手段５５０、ＲＯＭ（Read Only Memory）５６０、ＣＰＵ(Central Processing Unit)５７０、メモリ５８０、記録媒体５９５の記録媒体インタフェース（Ｉ／Ｆ）５９０を有し、これらはバス５１０によって相互に接続されている。

入出力Ｉ／Ｆ５２０は、ネットワーク等、外部から供給されるデジタル信号

を受信し、バス５１０上に出力するとともに、バス５１０上のデジタル信号を受信し、外部に出力する。コーデック５３０は、バス５１０を介して供給される例えばＭＰＥＧ符号化されたデータをデコードし、入出力Ｉ／Ｆ５４０に出力するとともに、入出力Ｉ／Ｆ５４０から供給されるデジタル信号をエンコードしてバス５１０上に出力する。入出力Ｉ／Ｆ５４０は、Ａ／Ｄ，Ｄ／Ａコンバータ５４１を内蔵している。入出力Ｉ／Ｆ５４０は、外部から供給されるアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ５４１でＡ／Ｄ(Analog Digital)変換することで、デジタル信号として、コーデック５３０に出力するとともに、コーデック５３０からのデジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ５４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

暗号処理手段５５０は、例えば、１チップのＬＳＩ(Large Scale Integrated Curcuit)で構成され、バス５１０を介して供給される例えばコンテンツ等のデジタル信号を暗号化し、または復号し、バス５１０上に出力する構成を持つ。なお、暗号処理手段５５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

ＲＯＭ５６０は、例えば、情報処理装置ごとに固有の、あるいは複数の情報処理装置のグループごとに固有のデバイスキーであるリーフキーと、複数の情報処理装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。ＣＰＵ５７０は、メモリ５８０に記憶されたプログラムを実行することで、コーデック５３０や暗号処理手段５５０等を制御する。

メモリ５８０は、上述したディスクＩＤリボケーションリスト（ＤＩＲＬ:Disc ID Revocation List）をディスクから読み取り格納する。ディスクＩＤリボケーションリスト（ＤＩＲＬ）はセキュアにメモリに格納する。例えば情報処理装置５００に設定されたＩＤに基づく暗号化を施してメモリに格納するなどにより耐タンパ性を保持したデータとして格納することが好ましい。

このようにディスクＩＤリボケーションリスト（ＤＩＲＬ）は外部から消されたり、内容を改ざんされたり、古いバージョンのリストに入れ替えられることを容易に実行されないように格納する。

メモリ５８０には、さらに、ＣＰＵ５７０が実行するプログラムや、ＣＰＵ５７０の動作上必要なデータを記憶する領域も含まれる。記録媒体インタフェース５９０は、デジタルデータを記録再生可能な記録媒体５９５を駆動することにより、記録媒体５９５からデジタルデータを読み出し（再生し）、バス５１０上に出力するとともに、バス５１０を介して供給されるデジタルデータを、記録媒体５９５に供給して記録させる。

記録媒体５９５は、例えば、ＤＶＤ、ＣＤ、ＭＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、記録媒体インタフェース５９０に対して着脱可能な構成であるとする。但し、記録媒体５９５は、情報処理装置５００に内蔵する構成としてもよい。

情報処理装置５００における情報記録媒体格納コンテンツの利用処理について、図１２～図１４のフローを参照して説明する。

図１２は、情報処理装置に図１を参照して説明した情報記録媒体をセットし、コンテンツ再生を開始する際に事前処理として実行される処理である。

ステップＳ１０１において、情報処理装置は、情報記録媒体に格納されたディスクＩＤリボケーションリスト（ＤＩＲＬ）を読み取り、正当性、すなわち改竄の有無の判定処理を行う。これは、前述したように、ディスクＩＤリボケーションリスト（ＤＩＲＬ）の改竄検証値として公開鍵暗号技術を用いたデジタル署名がなされている場合は、署名検証鍵（公開鍵）によって検証する。また、改竄検証値としてメッセージ認証コード（ＭＡＣ：Message Authentication

Code）が付与されている場合は、先に図３を参照して説明したＭＡＣ検証処理が実行される。

ディスクＩＤリボケーションリスト（ＤＩＲＬ）に改竄があると判定（ステップＳ１０２：Ｎｏ）されると、ステップＳ１０６に進み、その後の処理、すなわちコンテンツ再生を行うことなく処理を終了する。

ディスクＩＤリボケーションリスト（ＤＩＲＬ）に改竄がないと判定（ステップＳ１０２：Ｙｅｓ）されると、ステップＳ１０３に進み、情報記録媒体から読み出したディスクＩＤリボケーションリスト(ＤＩＲＬ)のバージョンと、情報処理装置のメモリに格納されているディスクＩＤリボケーションリスト（ＤＩＲＬ）とのバージョン比較を実行する。情報記録媒体から読み出したディスクＩＤリボケーションリスト（ＤＩＲＬ）のバージョンが情報処理装置に格納されているディスクＩＤリボケーションリスト（ＤＩＲＬ）より新しい場合は、ステップＳ１０５において、情報処理装置のメモリに情報記録媒体から読み出したディスクＩＤリボケーションリスト（ＤＩＲＬ）を書き込み、更新する。この処理により、情報処理装置のメモリには随時更新されたディスクＩＤリボケーションリスト（ＤＩＲＬ）が格納される。

なお、情報処理装置のメモリにディスクＩＤリボケーションリスト（ＤＩＲＬ）が未格納の場合には、バージョン比較を行うことなく、改竄検証のみを行い正当性の確認された情報記録媒体から読み出したディスクＩＤリボケーションリスト（ＤＩＲＬ）を情報処理装置のメモリに書き込む処理を実行する。

なお、上述した例では、ディスク上にディスクＩＤリボケーションリスト(ＤＩＲＬ）が格納されていて、それを用いて再生機のメモリのディスクＩＤリボケーションリスト（ＤＩＲＬ）を更新する例を説明したが、情報処理装置が電話回線やインターネット経由で管理局またはそこから委託されたサーバから最新のディスクＩＤリボケーションリスト（ＤＩＲＬ）を入手して更新しても

よいし、情報処理装置が製造される際に、その時点での最新のディスクＩＤリボケーションリスト(ＤＩＲＬ)をメモリに格納するようにしてもよい。また、たとえば家庭内でネットワークを構成している機器同士で互いに格納するディスクＩＤリボケーションリスト（ＤＩＲＬ）のバージョンを教えあい、新しいものを用いて古いものを更新するようにしてもよい。さらに、メディアが書き込み可能なメディアであれば、記録機器が最新バージョンのディスクＩＤリボケーションリスト（ＤＩＲＬ）を書き込み、それを用いてそのメディアを扱った機器のディスクＩＤリボケーションリスト（ＤＩＲＬ）を更新するようにしてもよい。

次に、図１３を参照して、情報処理装置が実行するリボーク判定処理について説明する。この処理は、図１２の処理に続いて実行する。ステップＳ２０１において、情報処理装置は、情報記録媒体から情報記録媒体ＩＤを読み出す。

ステップＳ２０２において、情報処理装置のメモリに格納したディスクＩＤリボケーションリスト（ＤＩＲＬ）のリボークＩＤリストと情報記録媒体から読み出した情報記録媒体ＩＤとの照合処理を実行する。

ステップＳ２０３において、ディスクＩＤリボケーションリスト(ＤＩＲＬ)のリボークＩＤリストと情報記録媒体から読み出した情報記録媒体ＩＤとが一致した場合は、ステップＳ２０４に進み、その後の処理、すなわちコンテンツ再生処理を実行することなく処理を終了する。

リボークＩＤリストと情報記録媒体から読み出した情報記録媒体ＩＤとが一致した場合は、上述の管理局（ＣＡ：Central Authority）が、不正流通ＣＤ－Ｒ等に基づいてコピーされた情報記録媒体ＩＤを抽出し、リボークＩＤリストにその情報記録媒体ＩＤを記述したものであることを意味する。従って、情報処理装置にセットされた情報記録媒体は、不正流通ＣＤ－Ｒ等であり、既に正当なコンテンツ利用権が失われた情報記録媒体またはそのコピーであり、

情報処理装置は、この情報記録媒体からのコンテンツ再生を実行することなく処理を終了する。

ステップＳ２０３において、ディスクＩＤリボケーションリスト（ＤＩＲＬ）のリボークＩＤリストと情報記録媒体から読み出した情報記録媒体ＩＤとが一致しなかった場合は、コンテンツ再生処理に移行する。

図１４を参照してコンテンツ再生処理シーケンスについて説明する。ステップＳ３０１において、情報処理装置は、情報記録媒体から、暗号鍵情報、すなわち有効化キーブロック（ＥＫＢ）を読み出す。ステップＳ３０２において、情報処理装置は、階層型キー配信構成によって予め情報処理装置に提供されているデバイスノードキー（ＤＮＫ）に基づいて有効化キーブロック（ＥＫＢ）の復号処理を実行して、コンテンツ鍵を取得する。この処理手順は、先に図６を参照して説明したとおりである。

ステップＳ３０３では、情報記録媒体から再生対象の暗号化コンテンツを読み出して、ステップＳ３０２で取得したコンテンツ鍵を用いてステップＳ３０４において復号し、再生する。ステップＳ３０５において、再生対象コンテンツがさらにある場合は、ステップＳ３０３，３０４の処理を繰り返し実行し、再生対象コンテンツが終了すると処理を終了する。

なお、また、コンテンツ鍵を導出する際に、ＥＫＢだけでなく、ディスク上に記録されている他の情報、たとえば、コンテンツのコピー制御情報などを適用してコンテンツ鍵を導出する構成としてもよい。また、ディスク製造業者がディスク製造時に、ディスク上に、ルートキーで暗号化したコンテンツ鍵を格納しておき、情報処理装置はこれを復号してコンテンツ鍵を得るようにしてもよい。

また、同一の情報記録媒体で、たとえばコンテンツが格納されているアドレ

スにより別個のコンテンツ鍵を用いてコンテンツを暗号化した構成も可能であり、この場合は、情報処理装置において、ステップＳ３０１～Ｓ３０４のコンテンツ鍵の導出、コンテンツの読み出し・復号を必要なだけ繰り返し実行する。

［４．情報記録媒体の製造、提供、管理構成］

次に、コンテンツを記録した情報記録媒体の製造、提供、管理構成について、図１５を参照して説明する。

図１５に示す例では、情報記録媒体製造業者６０３において、ＣＤ等の情報記録媒体６０４が製造されユーザの情報処理装置６０５において利用される。

図１を参照して説明したように、情報記録媒体には、暗号化コンテンツ、暗号鍵情報、情報記録媒体（ディスク）ＩＤ、情報記録媒体（ディスク）ＩＤリボケーションリスト（ＤＩＲＬ）とが格納される。

コンテンツプロバイダ６０２は、コンテンツを暗号化し、暗号化コンテンツとして情報記録媒体製造業者６０３に提供する。さらに、特定のユーザの持つデバイス（情報処理装置）の持つデバイスノードキー（ＤＮＫ）においてのみ処理可能な有効化キーブロック（ＥＫＢ）を情報記録媒体製造業者６０３に提供する。管理局（ＣＡ：Central Authority）６０１は、情報記録媒体（ディスク）ＩＤおよび、情報記録媒体（ディスク）ＩＤリボケーションリスト（ＤＩＲＬ）を情報記録媒体製造業者６０３に提供する。

情報記録媒体製造業者６０３は、コンテンツプロバイダ６０２から受領した暗号化コンテンツおよび有効化キーブロック（ＥＫＢ）と、管理局（ＣＡ：Central Authority）６０１から受領した情報記録媒体（ディスク）ＩＤおよび、情報記録媒体（ディスク）ＩＤリボケーションリスト（ＤＩＲＬ）を情報記録媒体に格納し情報記録媒体（ディスク）６０４を製造し、ユーザに提供す

る。ユーザは情報記録媒体（ディスク）６０４を情報処理装置６０５にセットして上述したコンテンツ利用処理を行う。

なお、デバイスノードキー(ＤＮＫ)のユーザ情報処理装置に対する提供は、管理局６０１またはコンテンツプロバイダ６０２のいずれが行ってもよい。あるいは図示しない他のサービスプロバイダが行ってもよい。

情報記録媒体製造装置の構成例について、図１６を参照して説明する。情報記録媒体製造装置７００は、入出力Ｉ／Ｆ(Interface)７２０、暗号処理手段７５０、ＲＯＭ(Read Only Memory)７６０、ＣＰＵ(Central Processing Unit)７７０、メモリ７８０、記録媒体７９５の記録媒体インタフェース（Ｉ／Ｆ）７９０を有し、これらはバス７１０によって相互に接続されている。

入出力Ｉ／Ｆ７２０は、外部から供給されるデジタル信号を受信し、バス７１０上に出力する。例えばコンテンツプロバイダからの暗号化コンテンツ、有効化キーブロック（ＥＫＢ）、および管理局（ＣＡ：Central Authority）から受領する情報記録媒体（ディスク）ＩＤおよび、情報記録媒体（ディスク）ＩＤリボケーションリスト（ＤＩＲＬ）などのデータをネットワークを介して受信することができる。なお、情報記録媒体（ディスク）ＩＤは、製造するディスクの数に応じた数のＩＤを管理局（ＣＡ：Central Authority）から受領する。

暗号処理手段７３０は、例えば、１チップのＬＳＩ(Large Scale Integrated Curcuit)で構成され、バス７１０を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス７１０上に出力する構成を持つ。コンテンツプロバイダかせ提供されるコンテンツが暗号化コンテンツでない場合には、暗号処理手段７３０において暗号化する。なお、暗号処理手段７５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。

メモリ７４０は、コンテンツプロバイダから受領した暗号化コンテンツおよび有効化キーブロック（ＥＫＢ）と、管理局（ＣＡ：Central Authority）から受領した情報記録媒体（ディスク）ＩＤおよび、情報記録媒体（ディスク）ＩＤリボケーションリスト（ＤＩＲＬ）とを格納する。なお、情報記録媒体（ディスク）ＩＤは、製造するディスクの数に応じた数のＩＤを管理局（ＣＡ：Central Authority）から受領しメモリ７４０に格納する。

コントローラ７５０は、情報記録媒体の製造プログラムに従った制御を実行する。ＣＰＵ等の制御部およびプログラム格納メモリを有する。コントローラ７５０の制御にしたがって、メモリ７４０に格納されたデータが、記録媒体に格納される。

記録媒体７７０は、例えば、ＤＶＤ、ＣＤ、ＭＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、記録媒体インタフェース７６０から記録データが供給されて記録格納される。

ディスクの製造処理手順について図１７を参照して説明する。図１７の処理は、情報記録媒体製造業者の情報記録媒体製造装置において実行する処理である。情報記録媒体製造装置には、上述したようにメモリが備えられ、メモリにコンテンツプロバイダから受領した暗号化コンテンツおよび有効化キーブロック（ＥＫＢ）と、管理局（ＣＡ：Central Authority）から受領した情報記録媒体（ディスク）ＩＤおよび、情報記録媒体（ディスク）ＩＤリボケーションリスト（ＤＩＲＬ）とが格納されているものとする。なお、情報記録媒体（ディスク）ＩＤは、製造するディスクの数に応じた数のＩＤを管理局（ＣＡ：Central Authority）から受領する。

ステップＳ４０１において、管理局（ＣＡ：Central Authority）から受領

し、メモリに格納済みの情報記録媒体（ディスク）ＩＤリボケーションリスト（ＤＩＲＬ）をメモリから読み出し、ステップＳ４０２、ステップＳ４０３において、コンテンツプロバイダから受領した有効化キーブロック（ＥＫＢ）、暗号化コンテンツをメモリから読み出し、ステップＳ４０４において、これらの情報を情報記録媒体(ディスク)に書き込んでマスターディスクを製造する。

次に、ステップＳ４０５において、マスターディスクに基づくスタンパによるスタンプ処理により、複製としてのディスクを製造する。次に、ステップＳ４０６において、管理局（ＣＡ：Central Authority）から受領し、メモリに格納済みの、ディスクＩＤを順次取り出してディスクに書き込む。ステップＳ４０７において、製造枚数が、管理局（ＣＡ：Central Authority）から受領したディスクＩＤ数に達した場合は、その時点でディスク製造を終了する。

このように、ディスク製造業者は、管理局（ＣＡ：Central Authority）から受領したディスクＩＤの数に応じて、それぞれの製造ディスクに異なるＩＤを格納する。

従って、市場に流通する情報記録媒体（ディスク）にはそれぞれ異なるＩＤが設定されていることになり、同一のディスクＩＤが設定されている複数のディスクが発見された場合は、不正なコピーが実行されているものと判断し、管理局（ＣＡ：Central Authority）が情報記録媒体（ディスク）ＩＤリボケーションリスト（ＤＩＲＬ）にそのディスクＩＤを書き込む更新処理を実行し、更新されたリストがディスク製造業者に提供され、新規ディスクには、そのリストが格納される。

更新リストを持つディスクを購入したユーザが、情報処理装置にディスクをセットし、コンテンツ再生処理を実行する際には、前述したように、情報処理装置内のメモリに格納された情報記録媒体（ディスク）ＩＤリボケーションリスト（ＤＩＲＬ）とのバージョン比較が実行され、更新されたリストがメモリ

に格納される。従って、ユーザの情報処理装置のメモリに格納されるリストは、随時更新される。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

例えば、プログラムは記憶媒体としてのハードディスクやＲＯＭ(Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記憶媒体に

インストールすることができる。

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

産業上の利用可能性

以上、説明したように、本発明の構成によれば、情報記録媒体に、暗号化コンテンツと、暗号化コンテンツの復号処理に必要とする暗号鍵情報と、情報記録媒体固有の識別子である情報記録媒体ＩＤと、不正であると判定された情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストとを格納した構成とし、情報記録媒体に格納されたコンテンツを読み出して再生する情報処理装置において、情報記録媒体に格納された情報記録媒体ＩＤが、情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと一致しないことを条件としてコンテンツ再生処理を実行する構成としたので、不正コピーコンテンツの格納媒体に記録された情報記録媒体ＩＤを情報記録媒体ＩＤリボケーションリストに記述することで、リスト化されたＩＤを持つディスクの再生が防止され、コンテンツの不正コピーの氾濫、利用を排除することが可能となる。

また、本発明の構成では、情報処理装置において、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストの改竄検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョン比較を実行し、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストのバージョンがメモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョンより新しいものである場合に、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストをメモリに格納するリスト更新処理を実行する構成としたので、随時更新されたリストによ

るコンテンツ再生制御の実行が可能となる。

請求の範囲

1． 情報記録媒体であり、

暗号化コンテンツと、

前記暗号化コンテンツの復号処理に必要とする暗号鍵情報と、

情報記録媒体固有の識別子である情報記録媒体ＩＤと、

不正であると判定された情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストと、

を格納したことを特徴とする情報記録媒体。

2． 前記情報記録媒体ＩＤリボケーションリストは、

該情報記録媒体ＩＤリボケーションリストの格納データの改竄の有無を判定するための改竄検証値を持つ構成であることを特徴とする請求項１に記載の情報記録媒体。

3． 前記暗号鍵情報は、

前記暗号化コンテンツの復号に適用する鍵を取得可能な暗号化鍵データとしての有効化キーブロック（ＥＫＢ：Enabling Key Block）を含む構成であることを特徴とする請求項１に記載の情報記録媒体。

4． 前記有効化キーブロック（ＥＫＢ：Enabling Key Block）は、

前記情報記録媒体の利用デバイスである情報処理装置に階層型鍵配信ツリー構成を適用して提供された鍵情報としてのデバイスノードキー（ＤＮＫ：Device Node Key）に基づいて復号処理の可能な暗号鍵情報であることを特徴とする請求項３に記載の情報記録媒体。

5． コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実行する情報処理装置であり、

不正であると判定された情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストを格納したメモリを有し、

情報記録媒体に格納された情報記録媒体ＩＤと前記メモリに格納された情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤとの照合処理を実行し、情報記録媒体に格納された情報記録媒体ＩＤが、情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと一致しないことを条件としてコンテンツ再生処理を実行する構成を有することを特徴とする情報処理装置。

６．　前記情報処理装置は、

情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストの改竄検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョン比較を実行し、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストのバージョンがメモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョンより新しいものである場合に、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストをメモリに格納するリスト更新処理を実行する構成であることを特徴とする請求項５に記載の情報処理装置。

７．　前記情報処理装置は、

階層型鍵配信ツリー構成を適用して提供された鍵情報としてのデバイスノードキー（ＤＮＫ：Device Node Key）を有し、

前記情報記録媒体に格納された暗号化鍵情報としての有効化キーブロック（ＥＫＢ：Enabling Key Block）を前記デバイスノードキー（ＤＮＫ：Device Node Key）に基づいて復号し、前記情報記録媒体に格納された暗号化コンテンツの復号に適用する鍵の取得処理を実行する構成であることを特徴とする請求項５に記載の情報処理装置。

８．　情報記録媒体を製造する情報記録媒体製造装置であり、

暗号化コンテンツと、

前記暗号化コンテンツの復号処理に必要とする暗号鍵情報と、

不正であると判定された情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストとを情報記録媒体に記録するとともに、

情報記録媒体固有の識別子である情報記録媒体ＩＤを製造する情報記録媒体毎に変更して記録する処理を実行する構成を有することを特徴とする情報記録媒体製造装置。

９．　前記情報記録媒体ＩＤリボケーションリストは、

該情報記録媒体ＩＤリボケーションリストの格納データの改竄の有無を判定するための改竄検証値を持つ構成であることを特徴とする請求項８に記載の情報記録媒体製造装置。

１０．　前記暗号鍵情報は、

前記暗号化コンテンツの復号に適用する鍵を取得可能な暗号化鍵データとしての有効化キーブロック（ＥＫＢ：Enabling Key Block）を含む構成であることを特徴とする請求項８に記載の情報記録媒体製造装置。

１１．　コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実行する情報処理方法であり、

情報記録媒体に格納された情報記録媒体ＩＤを読み出すステップと、

情報処理装置内のメモリに格納された不正情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと、前記情報記録媒体に格納された情報記録媒体ＩＤとの照合処理を実行するステップと、

情報記録媒体に格納された情報記録媒体ＩＤが、情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと一致しないことを条件としてコンテンツ再生処理を実行するステップと、

を有することを特徴とする情報処理方法。

１２．　前記情報処理方法は、さらに、

情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストの改竄検証処理を実行し、改竄のないことの判定を条件として、メモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョン比較を実行し、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストのバージョンがメモリに格納した情報記録媒体ＩＤリボケーションリストとのバージョンより新しいものである場合に、情報記録媒体に格納された情報記録媒体ＩＤリボケーションリストをメモリに格納するリスト更新処理を実行するステップを有することを特徴とする請求項１１に記載の情報処理方法。

１３．　前記情報処理方法は、さらに、

階層型鍵配信ツリー構成を適用して提供された鍵情報としてのデバイスノードキー（ＤＮＫ：Device Node Key）を適用して、前記情報記録媒体に格納された暗号化鍵情報としての有効化キーブロック（ＥＫＢ：Enabling Key Block）を復号し、前記情報記録媒体に格納された暗号化コンテンツの復号に適用する鍵の取得処理を実行するステップを有することを特徴とする請求項１１に記載の情報処理方法。

１４．　情報記録媒体を製造する情報記録媒体製造方法であり、

暗号化コンテンツと、前記暗号化コンテンツの復号処理に必要とする暗号鍵情報と、不正であると判定された情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストとを情報記録媒体に記録するステップと、

情報記録媒体固有の識別子である情報記録媒体ＩＤを製造する情報記録媒体毎に変更して記録する処理を実行するステップと、

を有することを特徴とする情報記録媒体製造方法。

１５．　コンテンツを格納した情報記録媒体からのコンテンツ再生処理を実行するコンピュータ・プログラムであり、

情報記録媒体に格納された情報記録媒体ＩＤを読み出すステップと、

情報処理装置内のメモリに格納された不正情報記録媒体ＩＤのリストである情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと、前記情報記録媒体に格納された情報記録媒体ＩＤとの照合処理を実行するステップと、

情報記録媒体に格納された情報記録媒体ＩＤが、情報記録媒体ＩＤリボケーションリストに記述されたリボーク情報記録媒体ＩＤと一致しないことを条件としてコンテンツ再生処理を実行するステップと、

を有することを特徴とするコンピュータ・プログラム。

THIS PAGE BLANK (USPTO)

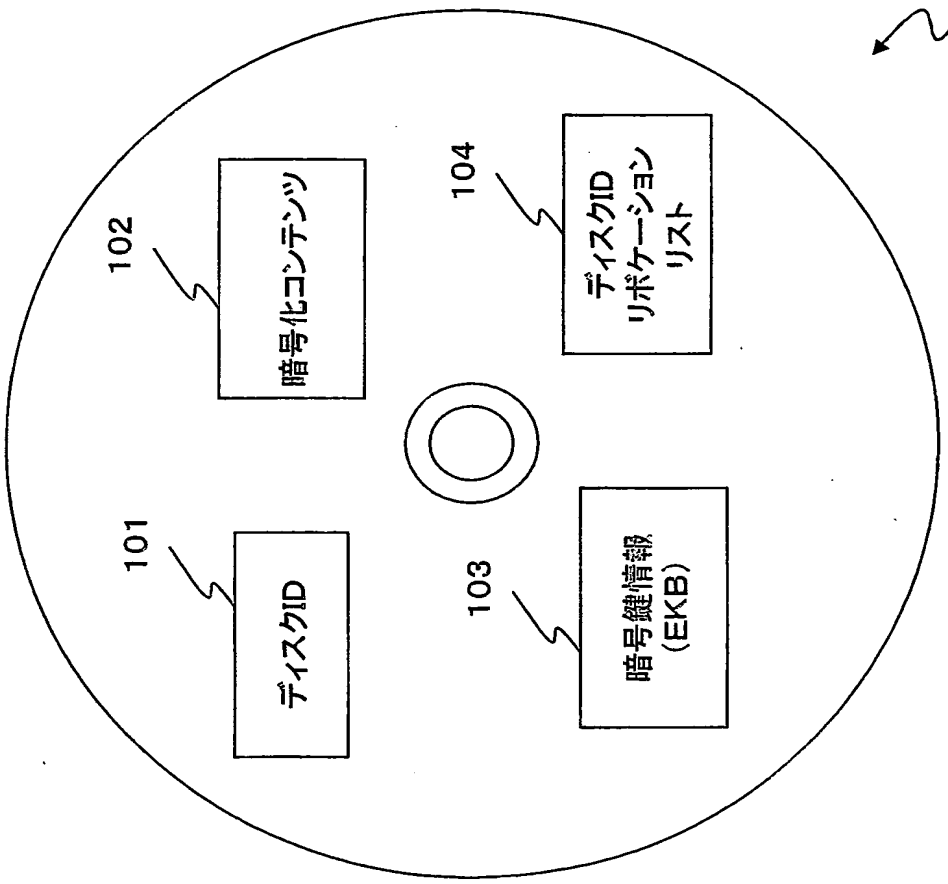
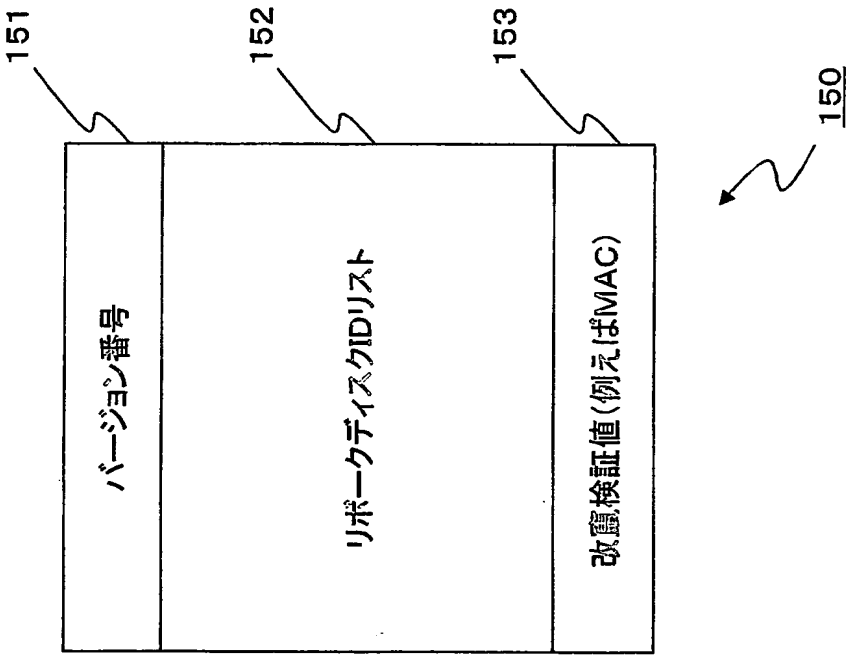

100
101
ディスクID
102
暗号化コンテンツ
103
暗号鍵情報
(EKB)
104
ディスクID
リボケーション
リスト

Fig. 1

SEP 2005

THIS PAGE BLANK (USPTO)

Fig.2



JC20 Rec'd PCT/PTO 22 SEP 2005

THIS PAGE BLANK (USPTO)

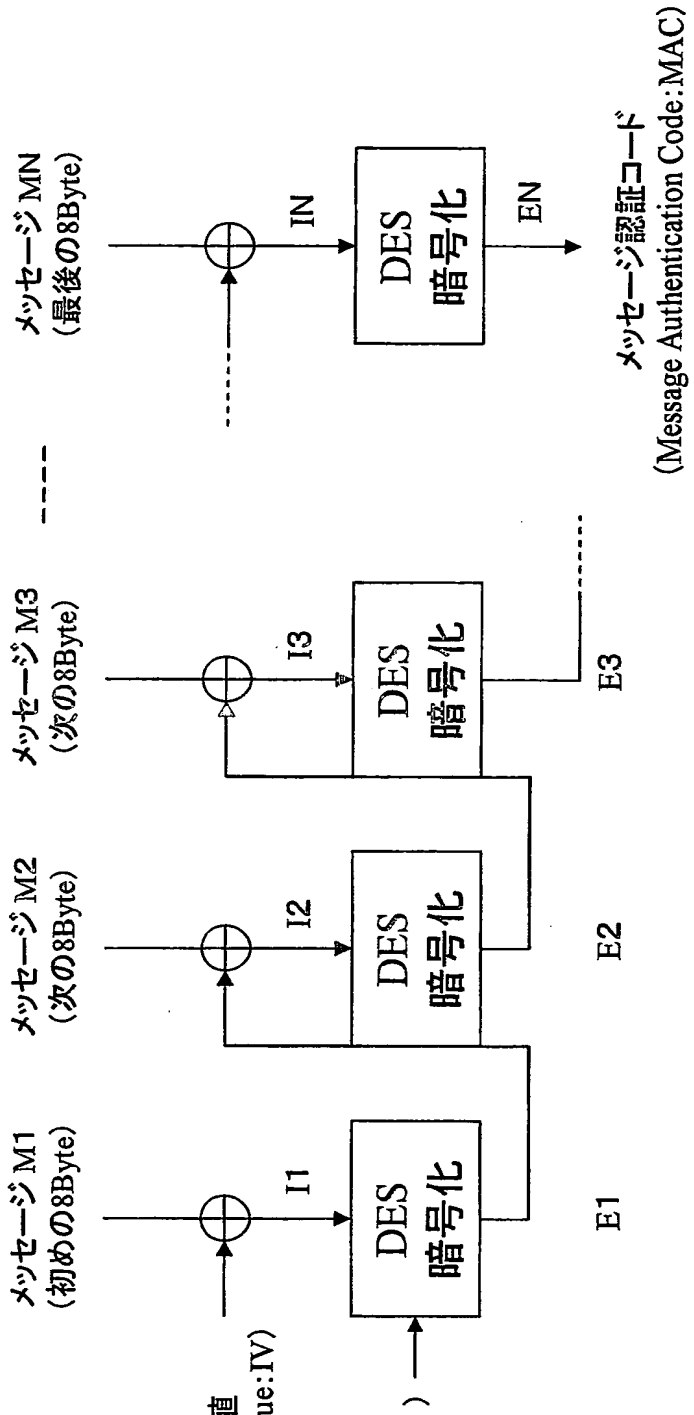
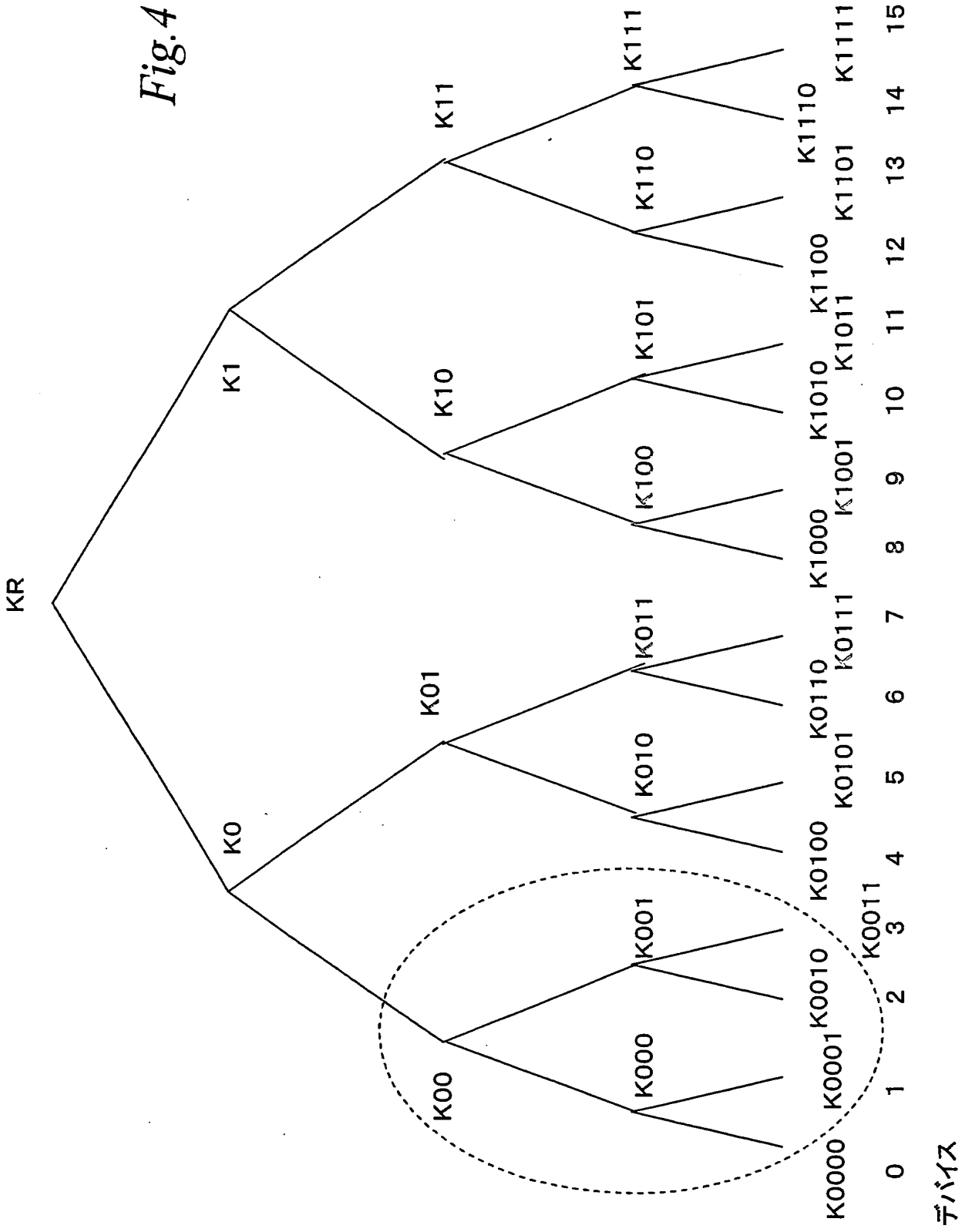

メッセージ M1
(初めの8Byte)
メッセージ M2
(次の8Byte)
メッセージ M3
(次の8Byte)
メッセージ MN
(最後の8Byte)
初期値
(Initial Value:IV)
鍵(K1)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
EN
メッセージ認証コード
(Message Authentication Code:MAC)
⊕ :排他的論理和処理(8バイト単位)

Fig.3

THIS PAGE BLANK (USPTO)

Fig.4


KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

THIS PAGE BLANK (USPTO)

(A) 有効化キーブロック
(EKB:Enabling Key Block)例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) 有効化キーブロック
(EKB:Enabling Key Block) 例2

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

Fig.5

THIS PAGE BLANK (USPTO)

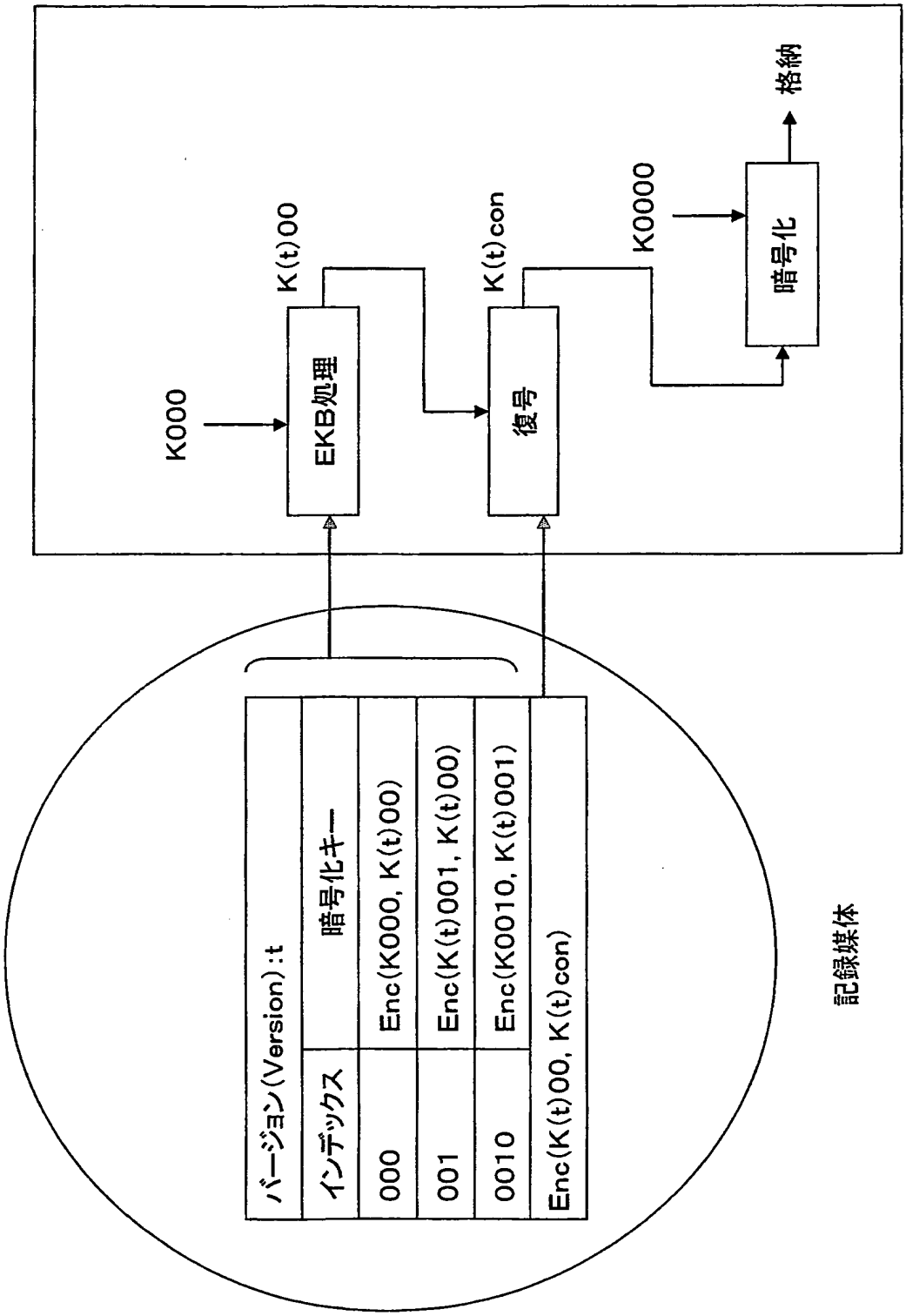
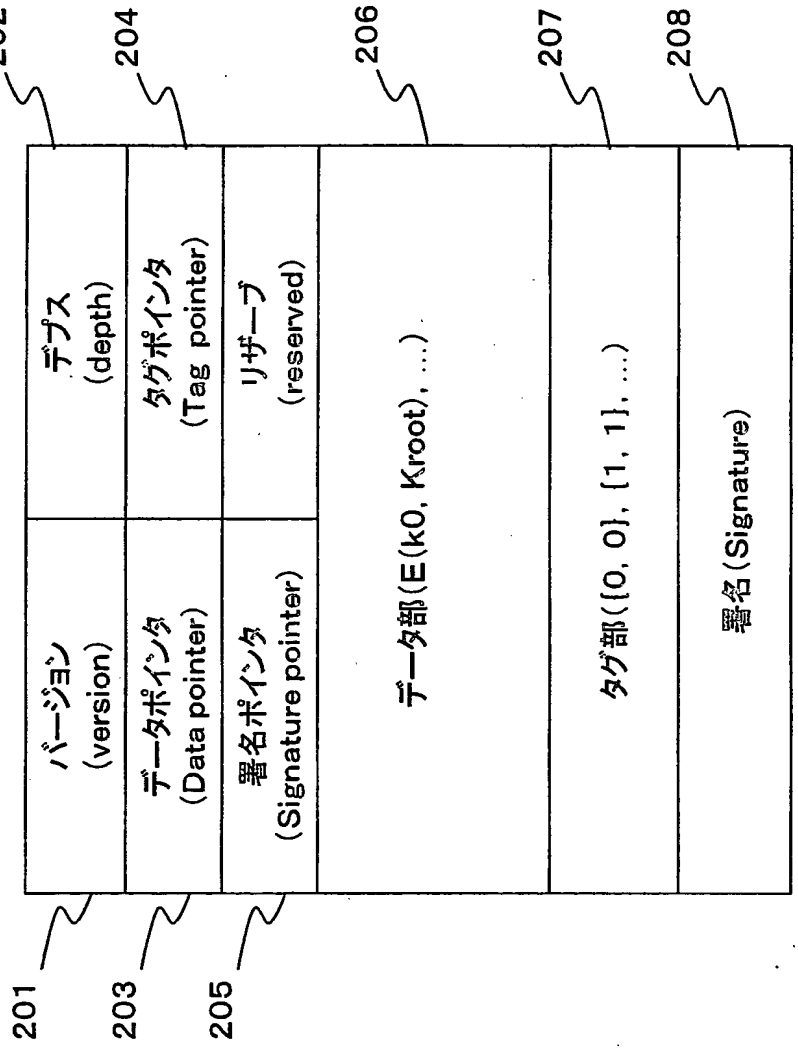

K000
EKB処理
K(t)00
復号
K(t)con
K0000
暗号化
格納
デバイス0
記録媒体
バージョン(Version):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)con)

Fig.6

JC20 Rec'd PCT/PTO 14 SEP 2005

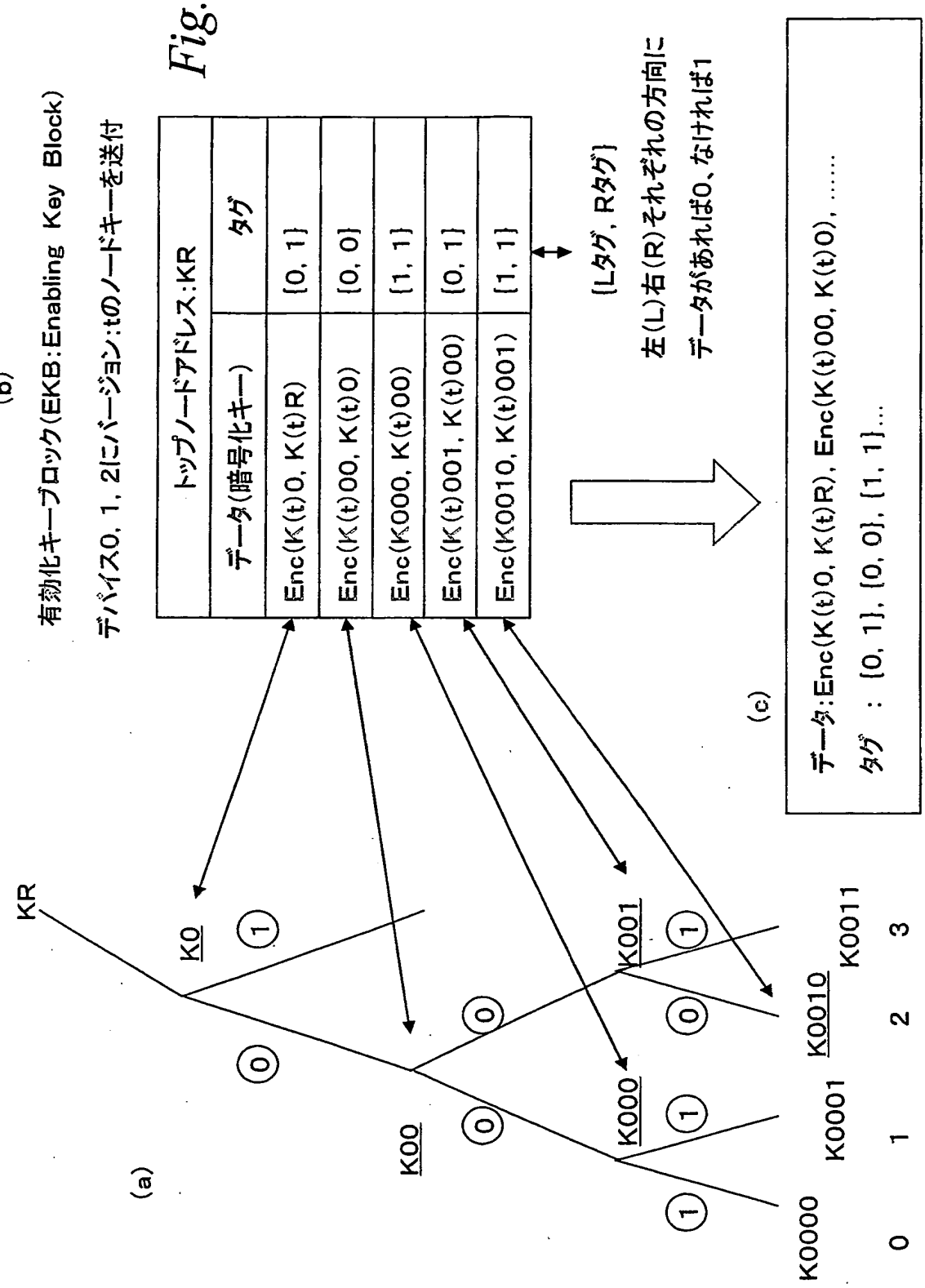
THIS PAGE BLANK (USPTO)

Fig.7


202
204
206
207
208
デプス (depth)
タグポインタ (Tag pointer)
リザーブ (reserved)
データ部(E(k0, Kroot), ...)
タグ部({0, 0}, {1, 1}, ...)
署名(Signature)
バージョン (version)
データポインタ (Data pointer)
署名ポインタ (Signature pointer)
201
203
205

THIS PAGE BLANK (USPTO)

Fig.8


(a)
KR
K0
K00
K000
K0000
K0001
K001
K0010
K0011
0
1
2
3
(b)
有効化キーブロック(EKB:Enabling Key Block)
デバイス0, 1, 2にバージョン:tのノードキーを送付
トップノードアドレス:KR
データ(暗号化キー)
タグ
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
{Lタグ, Rタグ}
左(L)右(R)それぞれの方向に
データがあれば0、なければ1
(c)
データ:Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0), ...
タグ : {0, 1}, {0, 0}, {1, 1}...

THIS PAGE BLANK (USPTO)

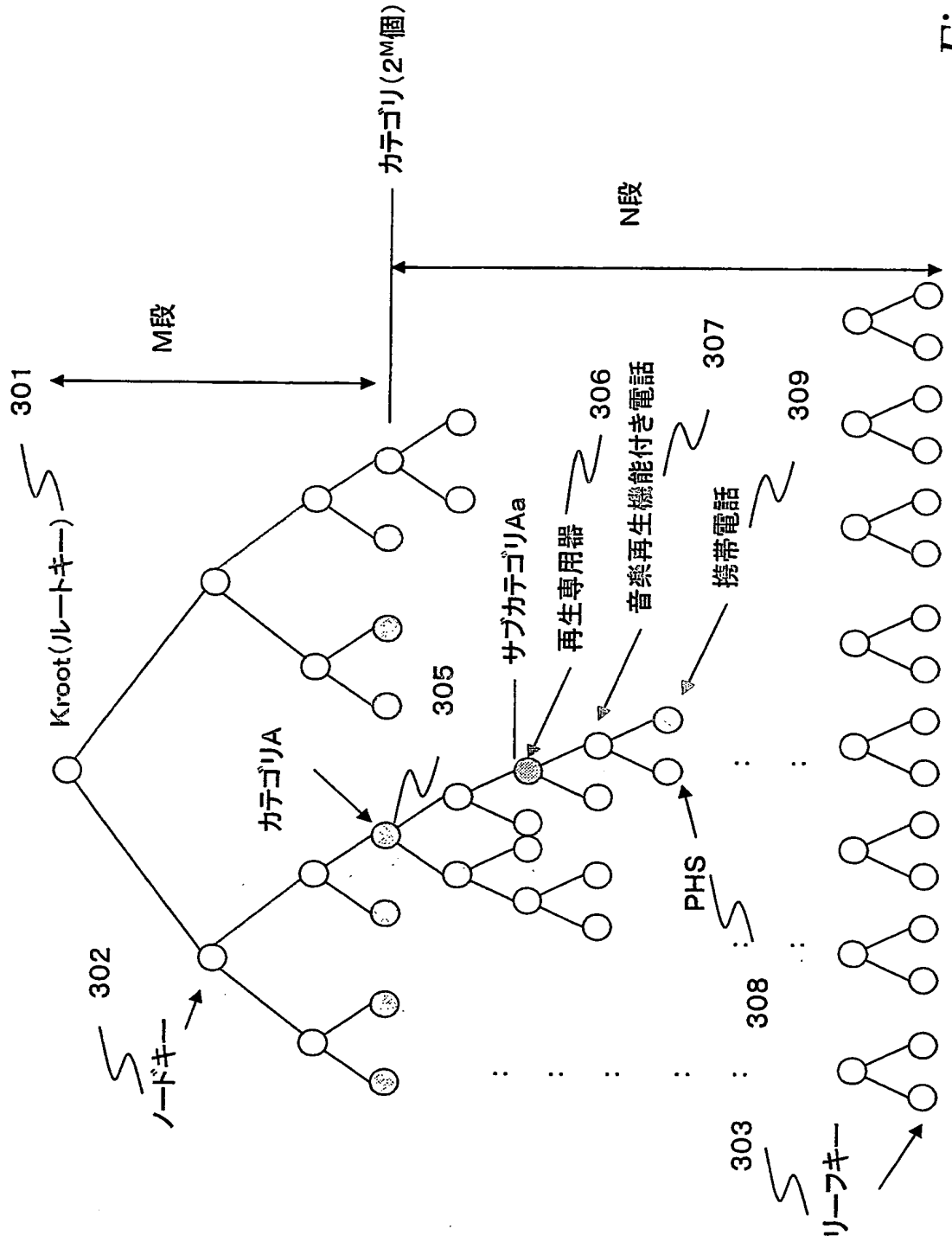
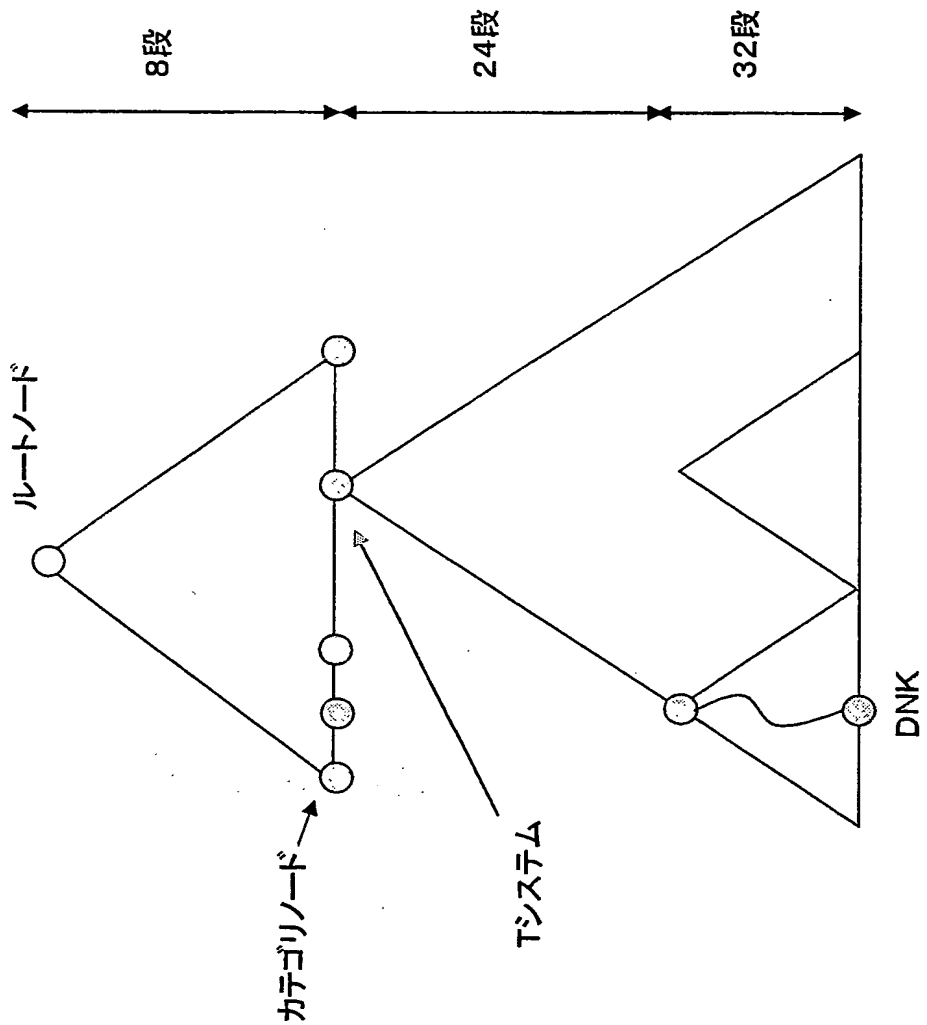

M段
N段
カテゴリ(2M個)
301
Kroot(ルートキー)
302
ノードキー
303
リーフキー
305
カテゴリA
サブカテゴリAa
306
再生専用器
307
音楽再生機能付き電話
309
携帯電話
PHS
308

Fig.9

JC20 Rec'd PCT/PTO 22 SEP 2005

THIS PAGE BLANK (USPTO)

Fig.10



THIS PAGE BLANK (USPTO)

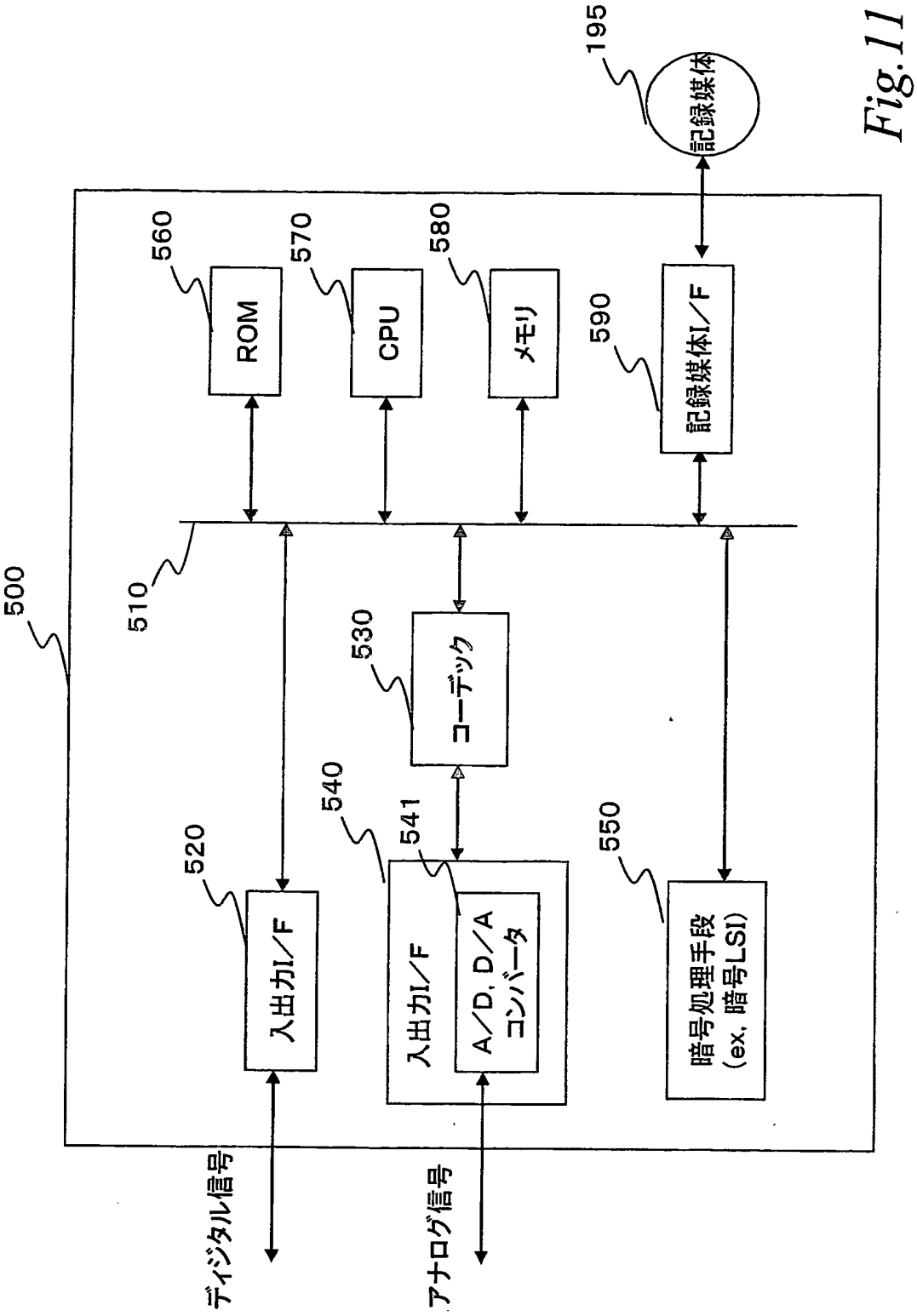

195
記録媒体
500
560
ROM
570
CPU
580
メモリ
590
記録媒体I／F
510
530
コーデック
540
541
A／D, D／A
コンバータ
520
入出力I／F
入出力I／F
550
暗号処理手段
(ex, 暗号LSI)
ディジタル信号
アナログ信号

Fig.11

THIS PAGE BLANK (USPTO)

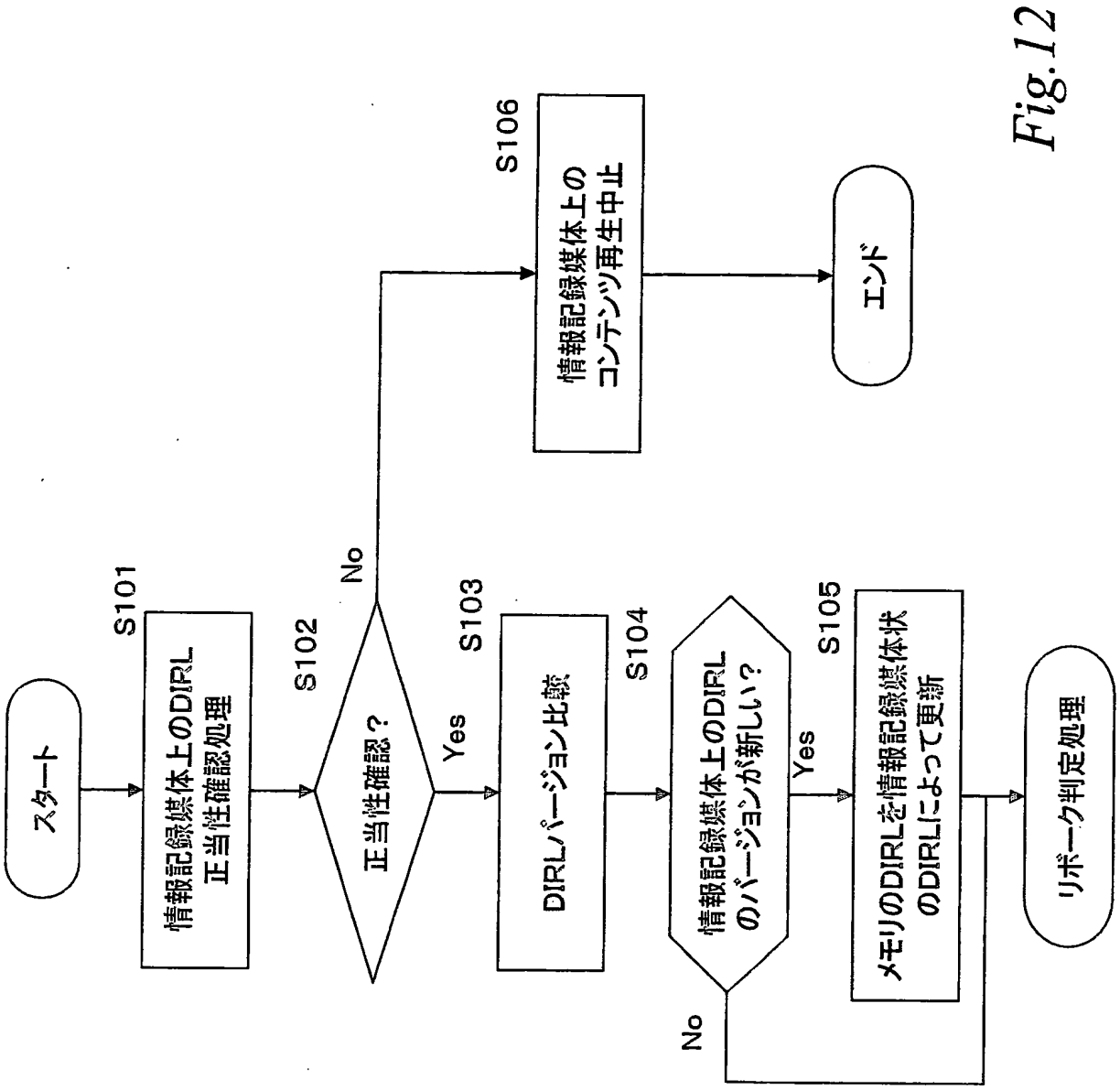

スタート
S101
情報記録媒体上のDIRL
正当性確認処理
S102
正当性確認？
No
Yes
S103
DIRLバージョン比較
S104
情報記録媒体上のDIRL
のバージョンが新しい？
No
Yes
S105
メモリのDIRLを情報記録媒体状
のDIRLによって更新
リボーク判定処理
S106
情報記録媒体上の
コンテンツ再生中止
エンド

Fig.12

JC20 Rec'd PCT/PTO 22 SEP 2005

THIS PAGE BLANK (USPTO)

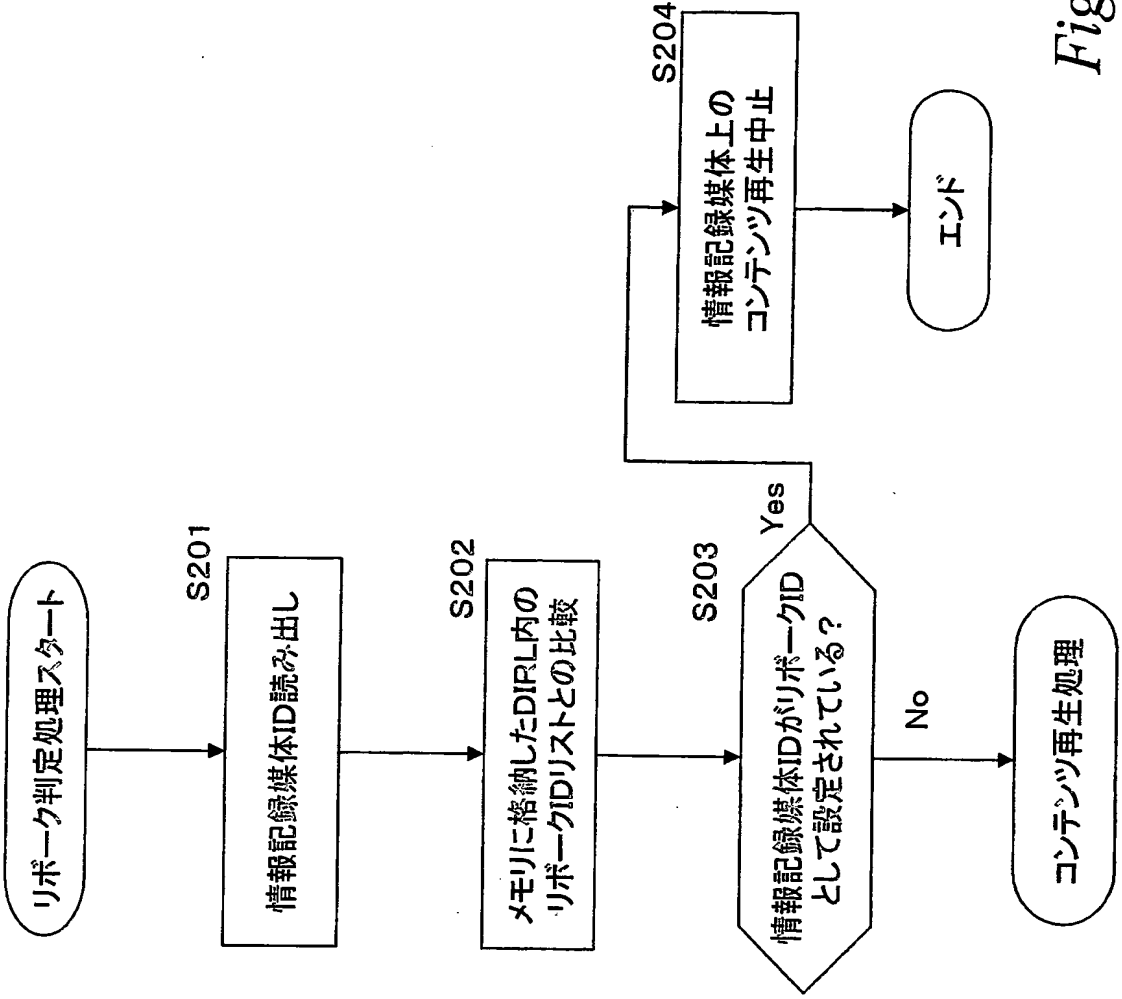
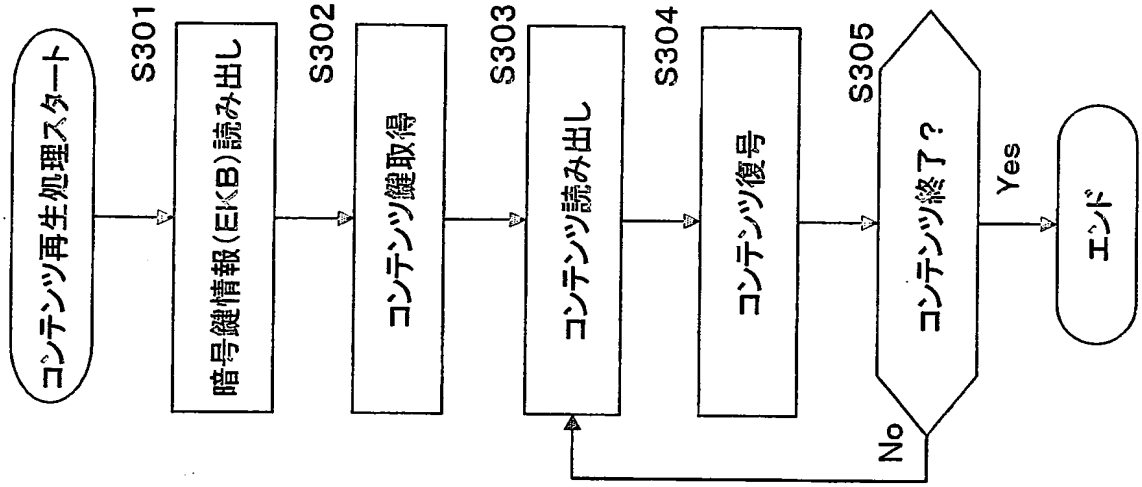

リボーク判定処理スタート
S201
情報記録媒体ID読み出し
S202
メモリに格納したDIRL内のリボークIDリストとの比較
S203
情報記録媒体IDがリボークIDとして設定されている？
Yes
No
S204
情報記録媒体上のコンテンツ再生中止
エンド
コンテンツ再生処理

Fig.13

THIS PAGE BLANK (USPTO)

Fig.14


コンテンツ再生処理スタート
S301
暗号鍵情報(EKB)読み出し
S302
コンテンツ鍵取得
S303
コンテンツ読み出し
S304
コンテンツ復号
S305
コンテンツ終了?
Yes
No
エンド

JC20 Rec'd PCT/PTO 22 SEP 2005

THIS PAGE BLANK (USPTO)

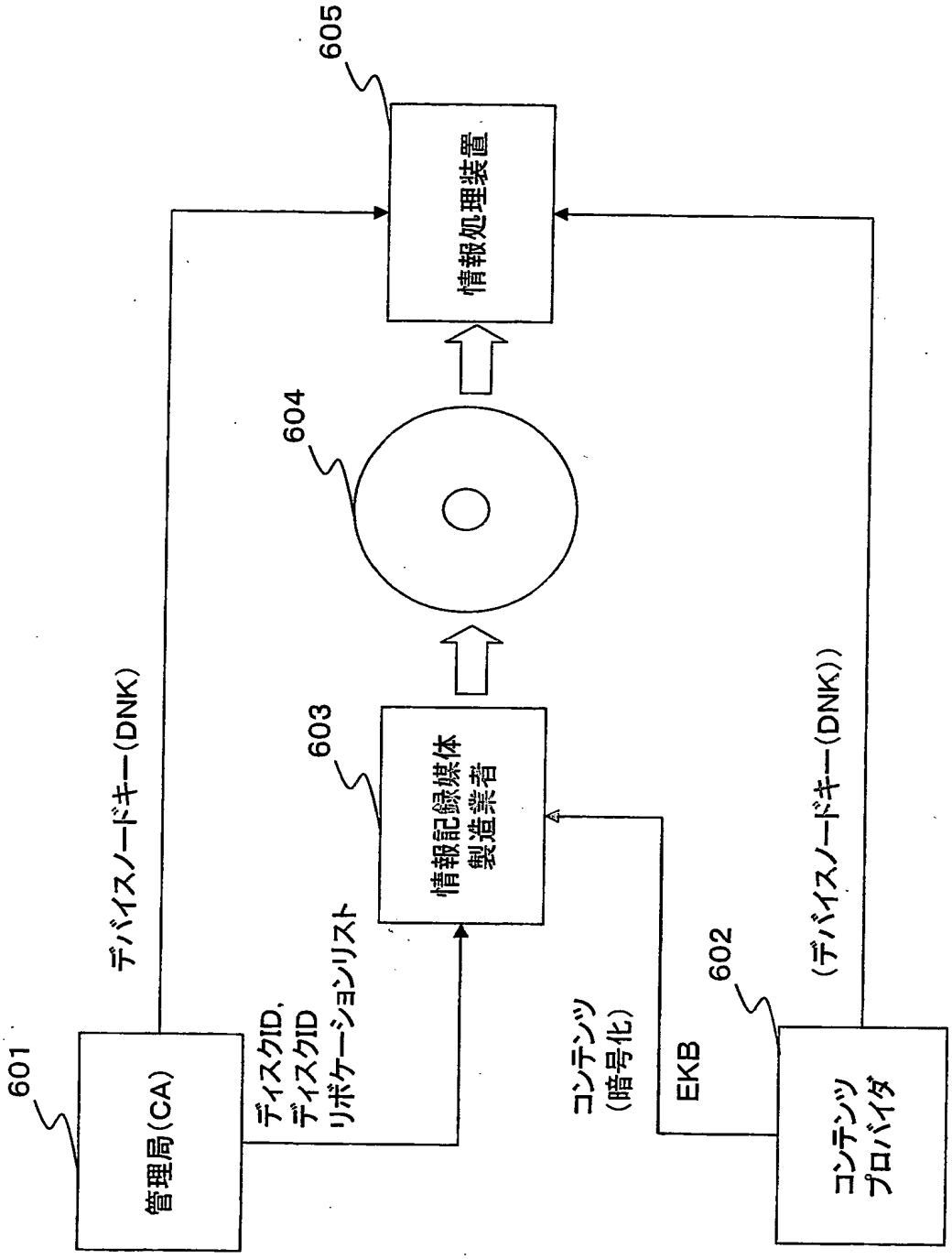

605
情報処理装置
604
603
情報記録媒体
製造業者
602
コンテンツ
プロバイダ
601
管理局(CA)
デバイスノードキー(DNK)
ディスクID,
ディスクID
リボケーションリスト
コンテンツ
(暗号化)
EKB
(デバイスノードキー(DNK))

Fig.15

JC20 Rec'd PCT/PTO 22 SEP 2005

THIS PAGE BLANK (USPTO)

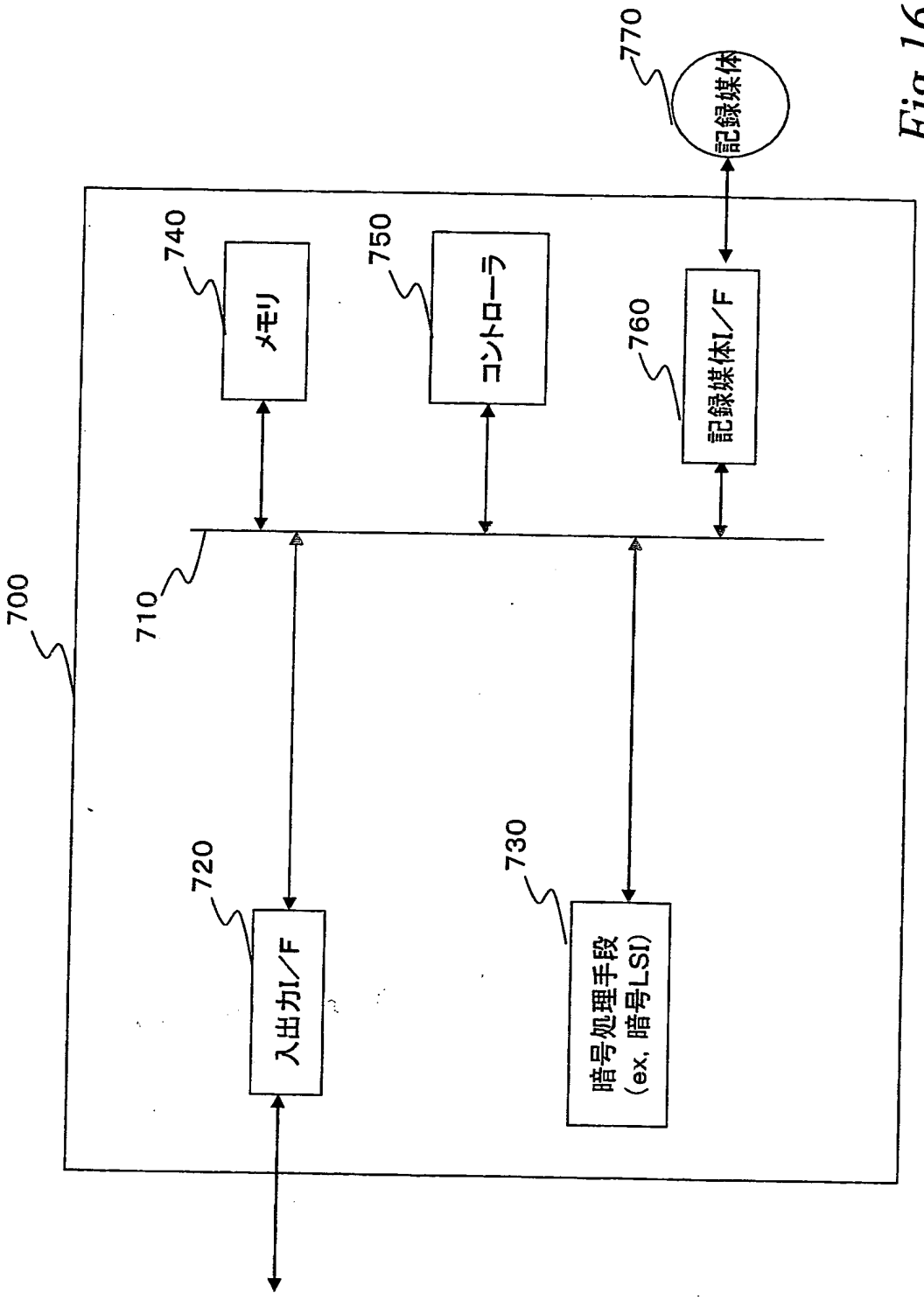

700
710
720
730
740
750
760
770
入出力I／F
暗号処理手段
(ex, 暗号LSI)
メモリ
コントローラ
記録媒体I／F
記録媒体

Fig.16

THIS PAGE BLANK (USPTO)

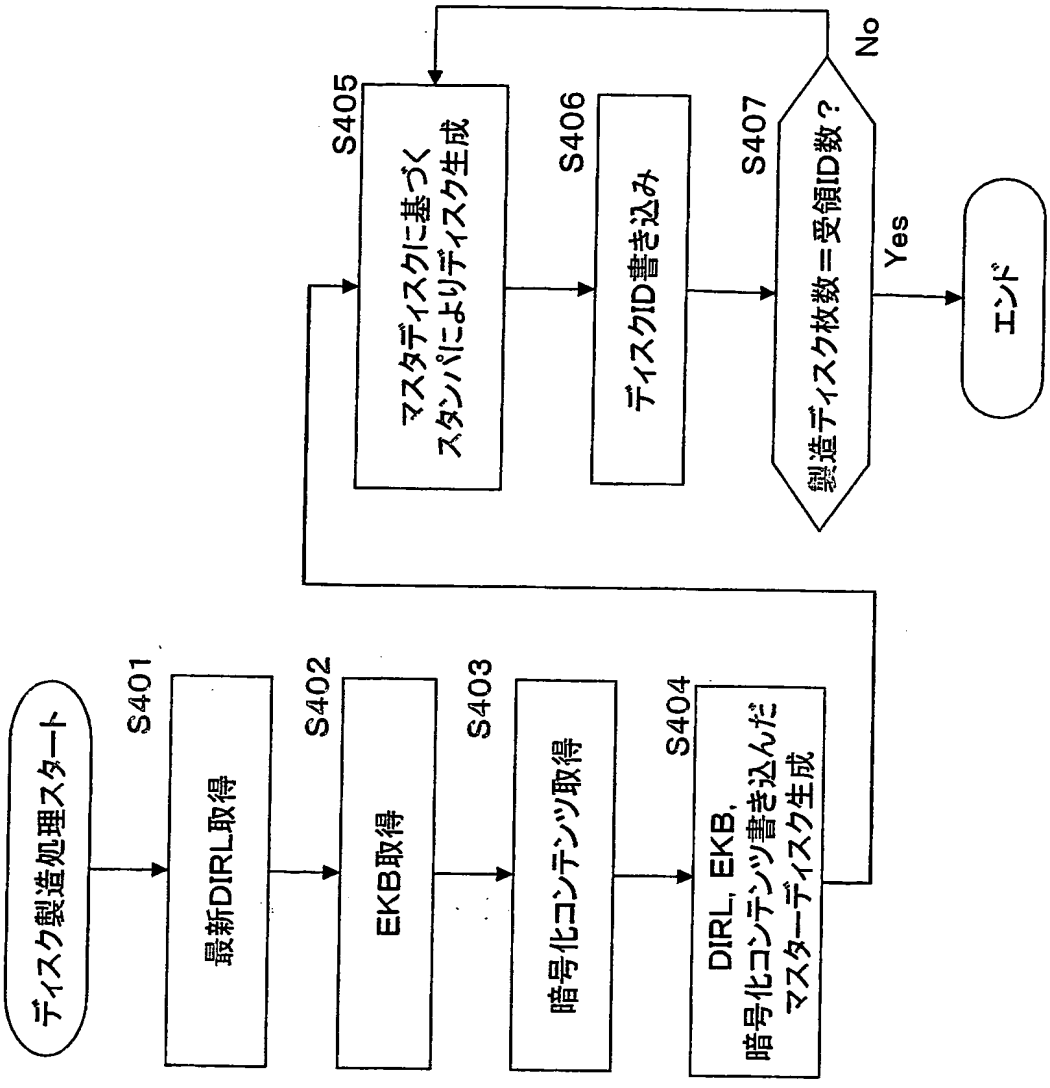

ディスク製造処理スタート
S401
最新DIRL取得
S402
EKB取得
S403
暗号化コンテンツ取得
S404
DIRL, EKB,
暗号化コンテンツ書き込んだ
マスターディスク生成
S405
マスタディスクに基づく
スタンパによりディスク生成
S406
ディスクID書き込み
S407
製造ディスク枚数＝受領ID数？
No
Yes
エンド

Fig. 17

JC20 Rec'd PCT/PTO 22 SEP 2005

THIS PAGE BLANK (USPTO)